H. Neuroth, A. Oßwald, R. Scheffel, S. Strathmann, K. Huth (Hrsg.)

# nestor Handbuch

## Eine kleine Enzyklopädie der digitalen Langzeitarchivierung

## Version 2.3

## Kapitel 5.2

## Grundkonzept der Vertrauenswürdigkeit und Sicherheit

nestor

nestor Handbuch: Eine kleine Enzyklopädie der digitalen Langzeitarchivierung
hg. v. H. Neuroth, A. Oßwald, R. Scheffel, S. Strathmann, K. Huth
im Rahmen des Projektes: nestor – Kompetenznetzwerk Langzeitarchivierung und Langzeitverfügbarkeit digitaler Ressourcen für Deutschland
nestor – Network of Expertise in Long-Term Storage of Digital Resources
http://www.langzeitarchivierung.de/

Kontakt: editors@langzeitarchivierung.de
c/o Niedersächsische Staats- und Universitätsbibliothek Göttingen,
Dr. Heike Neuroth, Forschung und Entwicklung, Papendiek 14, 37073 Göttingen

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet unter http://www.d-nb.de/ abrufbar.

Neben der Online Version 2.3 ist eine Printversion 2.0 beim Verlag Werner Hülsbusch, Boizenburg erschienen.

Die digitale Version 2.3 steht unter folgender Creative-Commons-Lizenz:
„Namensnennung-Keine kommerzielle Nutzung-Weitergabe unter gleichen Bedingungen 3.0 Deutschland“
http://creativecommons.org/licenses/by-nc-sa/3.0/de/

Markenerklärung: Die in diesem Werk wiedergegebenen Gebrauchsnamen, Handelsnamen, Warenzeichen usw. können auch ohne besondere Kennzeichnung geschützte Marken sein und als solche den gesetzlichen Bestimmungen unterliegen.

URL für Kapitel 5.2 „Grundkonzept der Vertrauenswürdigkeit und Sicherheit“ (Version 2.3):
urn:nbn:de:0008-2010030597
http://nbn-resolving.de/urn/resolver.pl?urn=urn:nbn:de:0008-2010030597

*Gewidmet der Erinnerung an Hans Liegmann (†), der als Mitinitiator und früherer Herausgeber des Handbuchs ganz wesentlich an dessen Entstehung beteiligt war.*

## 5.2 Grundkonzepte der Vertrauenswürdigkeit und Sicherheit

*Susanne Dobratz und Astrid Schoger*

Der Begriff der Vertrauenswürdigkeit digitaler Langzeitarchive wird von bewährten Konzepten der Vertrauenswürdigkeit von IT-Systemen abgeleitet. Im Internet Security Glossary[1] wird Vertrauenswürdigkeit (engl. trustworthiness) als die Eigenschaft eines Systems definiert, gemäß seinen Zielen und Spezifikationen zu operieren (d.h. es tut genau das, was es zu tun vorgibt) und dies auch in geeigneter Weise glaubhaft zu machen (z.B. durch eine formale Analyse). Die Common Criteria[2] führen Vertrauenswürdigkeit folgendermaßen ein:

„Werte" an deren Erhaltung „Eigentümer" Interesse haben, sind durch „Risiken"[3] bedroht. Zur Minimierung dieser Risiken werden „Gegenmaßnahmen" eingesetzt. Die Prüfung und Bewertung der eingesetzten Maßnahmen erbringt den Nachweis der „Vertrauenswürdigkeit". Vgl. dazu nachfolgende Abbildungen.

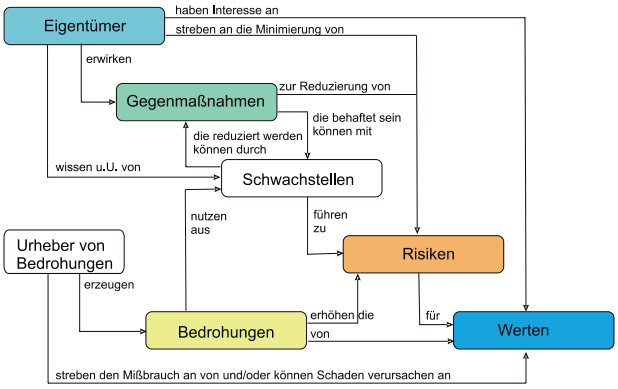


*Abbildung 1: Konzept der Bedrohungen und Risiken gemäß Common Criteria (Quelle: BSI 2006)*

1 Network Working Group (2007): "trusted system: a system that operates as expected,according to design and policy, doing what is required; trustworthy system: a system that not only is trusted, but also warrants that trust because the system's behavior can be validated in some convincing way, such as through formal analysis or code review." Alle hier aufgeführten URLs wurden im Mai 2010 auf Erreichbarkeit geprüft.

2 BSI (2006)

3 Vgl. dazu auch Howard (1998)

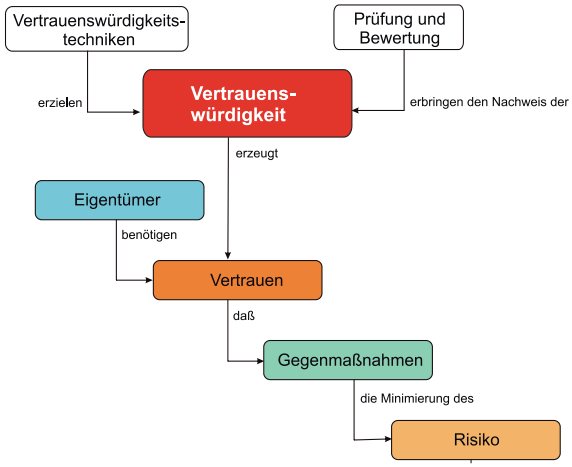


*Abbildung 2: Vertrauenswürdigkeitskonzept gemäß den Common Criteria (Quelle: BSI 2006)*

Ziel der digitalen Langzeitarchivierung ist der Erhalt der Informationen, die durch digitale Objekte repräsentiert sind.

Im Sinne der Langzeitarchivierung stellen Information den zu erhaltenden „Wert" dar. Informationen, die durch digitale Objekte repräsentiert werden, sind bedroht durch Einbußen in ihrer Integrität, Authentizität und Vertraulichkeit sowie den gänzlichen Verlust der Verfügbarkeit und Nutzbarkeit. Diese Eigenschaften bilden eine Teilmenge des Gesamtkonzeptes Sicherheit in der Informatik, wie sie u. a. in Steinmetz (2002) beschrieben sind:

- Integrität: sagt aus, ob die digitalen Objekte unverändert vorliegen,
- Authentizität: bezieht sich auf die Echtheit der digitalen Objekte, insbesondere den Aspekt der Nachweisbarkeit der Identität des Erstellers (Urhebers, Autors),
- Vertraulichkeit: bezieht sich darauf, dass unberechtigten Dritten kein Zugang zu den digitalen Objekten gewährleistet wird,
- Verfügbarkeit: bezieht sich auf den Aspekt der Zugänglichkeit zum digitalen Objekt.

Gemäß OAIS[4] wird unter einem digitalen Langzeitarchiv eine Organisation (bestehend aus Personen und technischen Systemen) verstanden, die die Verantwortung für den Langzeiterhalt und die Langzeitverfügbarkeit digitaler Objekte sowie für ihre Interpretierbarkeit zum Zwecke der Nutzung durch eine bestimmte Zielgruppe übernommen hat. Dabei bedeutet „Langzeit" über Veränderungen in der Technik (Soft- und Hardware) hinweg und auch unter

4 Vgl. dazu CCSDS (2002) sowie Kapitel 4 dieses Handbuchs

Berücksichtigung möglicher Änderungen der Zielgruppe.

Aus dem Ziel der Langzeitarchivierung lassen sich folgende zentrale Aufgaben eines digitalen Langzeitarchivs ableiten: Aufnahme (Ingest), Archivablage (Archival Storage), Nutzung (Access); ferner unterstützende Aufgaben wie das Datenmanagement und die Administration des Gesamtsystems. Besondere Bedeutung kommt der strategischen Planung (Preservation Planning) und Durchführung der Langzeiterhaltungsmaßnahmen[5], die die Langzeitverfügbarkeit und Interpretierbarkeit (d.h. der Rekonstruierbarkeit der darin enthaltenen Informationen) sicherstellen, zu. [6]

Diese Aufgaben stellen die Grundlage für die Spezifikation von Anforderungen an digitale Langzeitarchive dar, wie bereits 2002 im Bericht[7] der RLG/OCLC Working Group on Digital Archive Attributes aufgeführt. Die RLG-NARA Task Force on Digital Repository Certification hat 2007 (als Entwurf zur öffentlichen Kommentierung bereits 2006) eine Liste von Kriterien „Trustworthy Repositories Audit and Certification: Criteria and Checklist (TRAC)“[8] erarbeitet, die ein vertrauenswürdiges digitales Langzeitarchiv erfüllen muss. Diese Liste dient der Orientierung beim Auf- und Ausbau digitaler Langzeitarchive und kann als Checkliste auch zur Selbstevaluierung sowie zum externen Audit eingesetzt werden.

nestor hat unter Berücksichtigung nationaler Ansätze und Arbeitsergebnisse wie des „DINI-Zertifikats für Dokumenten- und Publikationsserver“[9] sowie den oben genannten internationalen Arbeiten Kriterien entwickelt, die den speziellen Bedürfnissen der deutschen Gedächtnisorganisationen Rechnung tragen. Diese wurden zunächst im Sommer 2006 als Entwurf zur öffentlichen Kommentierung publiziert und dank der vielfältigen Rückmeldungen der Anwender gründlich überarbeitet und liegen nun in Version 2 vor.[10]

Eine Prüfung und Bewertung digitaler Langzeitarchive gemäß dieser Kriterienkataloge kann somit den Nachweis der Vertrauenswürdigkeit erbringen. Die Grundprinzipien der Kriterienkataloge sowie deren Inhalte werden in Kapitel 5.4 anhand des nestor-Kriterienkataloges genauer erörtert.

Im Rahmen des EU-Projektes DigitalPreservationEurope (DPE) in Zusammenarbeit mit dem Digital Curation Centre (DCC) wurde das Tool „Digital

5 Vgl. dazu Kapitel 8 dieses Handbuchs
6 Vgl. dazu das Funktionsmodell des OAIS-Referenzmodells
7 RLG/OCLC (2002)
8 RLG/NARA (2007)
9 DINI (2007)
10 nestor AG Vertrauenswürdige Archive - Zertifizierung (2008)

Repository Audit Method based on Risk Assessment (DRAMBORA)“[11] zur Selbstevaluierung entwickelt, das die Risikoanalyse als Methode einsetzt. Ausgehend von den Zielen eines digitalen Langzeitarchivs müssen zunächst die Aktivitäten spezifiziert und die damit verbundenen Werte identifiziert werden. In einem weiteren Schritt werden dann die Risiken aufgedeckt und die zu deren Minimierung eingesetzten Maßnahmen bewertet.

Somit wird ein anderer Weg zum Nachweis der Vertrauenswürdigkeit beschrieben.

## Internationale Kooperation, Standardisierung und Zertifizierung – 10 gemeinsame Prinzipien

Bevor ein international abgestimmtes Zertifizierungsverfahren für digitale Langzeitarchive entwickelt werden kann, ist es zunächst wichtig, einen internationalen Konsens über die Evaluierungskriterien zu finden. Ferner müssen aus den Erfahrungen mit der Anwendung der Kriterienkataloge und Evaluierungstools Bewertungsmaßstäbe für unterschiedliche Typen von digitalen Langzeitarchiven ausgearbeitet werden.

Wesentliche Vertreter des Themas Vertrauenswürdigkeit auf internationaler Ebene - Center for Research Libraries (CRL), Digital Curation Centre (DCC), Projekt DigitalPreservationEurope (DPE) sowie nestor haben 10 gemeinsame Prinzipien[12] herausgearbeitet, die den oben genannten Kriterienkatalogen und Audit Checklisten zu Grunde liegen. Diese stellen die Grundlage der weiteren inhaltlichen Zusammenarbeit dar. Die 10 Kriterien lauten wie folgt[13]:

1. Das digitale Langzeitarchiv übernimmt die Verantwortung für die dauerhafte Erhaltung und kontinuierliche Pflege der digitalen Objekte für die identifizierten Zielgruppen.
2. Das digitale Langzeitarchiv belegt die organisatorische Beständigkeit (auch in den Bereichen Finanzierung, Personalausstattung, Prozesse), um seine Verantwortung zu erfüllen.
3. Das digitale Langzeitarchiv verfügt über die erforderlichen Rechte (per Vertrag oder Gesetz), um seine Verantwortung zu erfüllen.
4. Das digitale Langzeitarchiv besitzt ein effektives und effizientes Geflecht von Grundsätzen (policy).
5. Das digitale Langzeitarchiv erwirbt und übernimmt digitale Objekte auf der Grundlage definierter Kriterien gemäß seinen Verpflichtungen und

11 DCC/DPE (2008)

12 CRL/DCC/DPE/nestor (2007)

13 nestor-Übersetzung

Fähigkeiten.

6. Das digitale Langzeitarchiv stellt die Integrität, Authentizität und Nutzbarkeit der dauerhaft aufbewahrten Objekte sicher.
7. Das digitale Langzeitarchiv dokumentiert alle Maßnahmen, die während des gesamten Lebenszyklus auf die digitalen Objekte angewendet werden, durch angemessene Metadaten.
8. Das digitale Langzeitarchiv übernimmt die Bereitstellung der digitalen Objekte.
9. Das digitale Langzeitarchiv verfolgt eine Strategie zur Planung und Durchführung von Langzeiterhaltungsmaßnahmen.
10. Das digitale Langzeitarchiv besitzt eine angemessene technische Infrastruktur zur dauerhaften Erhaltung und Sicherung der digitalen Objekte.

Sowohl die Kriterienkataloge als auch das Verfahren DRAMBORA werden zur Zeit der nationalen sowie internationalen Standardisierung zugeführt. Im Rahmen des DIN kümmert sich der neu gegründete Arbeitskreis „Vertrauenswürdige digitale Archive“ im Rahmen des NABD15 „Schriftgutverwaltung und Langzeitverfügbarkeit digitaler Informationsobjekte“ um die Vorbereitung einer deutschen Norm[14] für diesen Bereich. Dieser Arbeitskreis arbeitet eng zusammen mit den entsprechenden Ausschüssen der ISO und zwar dem TC46/SC11, der mit dem Entwurf „Risk assessment for records systems” die Normungsarbeit an DRAMBORA übernommen hat sowie dem TC20/SC13, der „TRAC: Trustworthy Repositories Audit and Certification: Criteria and Checklist“ einer Normierung zuführt.

Weitere Fachgemeinschaften haben sich auf der Grundlage dieser Vorarbeiten entschieden, eigene, für ihre jeweiligen Fachgebiete angepasste, Kriterien in Form von Katalogen aufzu-stellen, so z.B. die Europäische Ground Segment Coordination Body (GSCB)[15] oder das Data Seal of Approval[16].

Die Anwendung von Konzepten der IT-Sicherheit wie Hashfunktionen, Fingerprintingverfahren und digitalen Signaturen, kann bestimmte Risiken, die den Erhalt digitaler Objekte bedrohen, minimieren, insbesondere jene, welche die Integrität, Authentizität und Vertraulichkeit digitaler Objekte betreffen. Von besonderer Bedeutung für die Langzeitarchivierung ist der „Langzeit“-Aspekt, so dass bei allen eingesetzten Methoden die Nachhaltigkeit besonders geprüft werden muss. Diese Verfahren werden im nachfolgenden Kapitel dargestellt.

---

14 DIN 31644: Information und Dokumentation - Kriterienkatalog für vertrauenswürdige digitale Langzeitarchive

15 GSCB (2009)

16 Data Seal of Approval (2009)

## Literatur

Network Working Group (2007): *Internet Security Glossary. Request for Comments: 4949* http://tools.ietf.org/html/rfc4949

BSI Bundesamt für Sicherheit in der Informationstechnik (2006): *Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, Common Criteria* V 3.1, https://www.bsi.bund.de/cln_183/ContentBSI/Themen/ZertifizierungundAkkreditierung/ZertifierungnachCCundITSEC/ITSicherheitskriterien/CommonCriteria/cc.html

Howard, John D. / Longstaff, Thomas A. (1998): *A Common Language for Computer Security Incidents*. SANDIA Reports SAND98-8667. Albuquerque, New Mexico : Sandia National Laboratories http://www.cert.org/research/taxonomy_988667.pdf

CCSDS (Consultative Committee for Space Data Systems) (2002*): Reference Model for an Open Archival Information System (OAIS). Blue Book.* http://www.ccsds.org/docu/dscgi/ds.py/Get/File-143/650x0b1.pdf entspricht ISO 14721:2003

RLG/OCLC Working Group on Digital Archive Attributes (2002): *Trusted Digital Repositories: Attributes and Responsibilities*, http://www.oclc.org/programs/ourwork/past/trustedrep/repositories.pdf

DINI Deutsche Initiative für Netzwerkinformation / AG Elektronisches Publizieren (2007): *DINI-Zertifikat für Dokumenten- und Publikationsservice 2007*. DINI-Schriften 3. http://nbn-resolving.de/urn:nbn:de:kobv:11-10079197

nestor Arbeitsgruppe Vertrauenswürdige Archive – Zertifizierung (2008): *nestor-Kriterien: Kriterienkatalog vertrauenswürdige digitale Langzeitarchive.* Version 2. Frankfurt am Main : nestor http://nbn-resolving.de/urn:nbn:de:0008-2008021802

Steinmetz, Ralf (2000) : *Multimedia-Technologie: Grundlagen, Komponenten und Systeme*, 3. Auflage , Berlin, Heidelberg, New York : Springer

DCC Digital Curation Centre / DPE Digital Preservation Europe (2008): *Digital Repository Audit Method Based on Risk Assessment (DRAMBORA), interactive,* http://www.repositoryaudit.eu/

CRL Center for Research Libraries / DCC Digital Curation Centre / DPE Digital Preservation Europe / nestor (2007): *Core Requirements for Digital Archives*, http://www.crl.edu/archiving-preservation/digital-archives/metrics-assessing-and-certifying/core-re

Data Seal of Approval (2009): Guidelines http://www.datasealofapproval.org/?q=node/35

GSCB Ground Segment Coordination Body (2009): Long Term Preservation of Earth obser-vation Space-Data - European LTDP Common Guidelines http://earth.esa.int/gscb/ltdp/EuropeanLTDPCommonGuidelines_Issue1.0.pdf