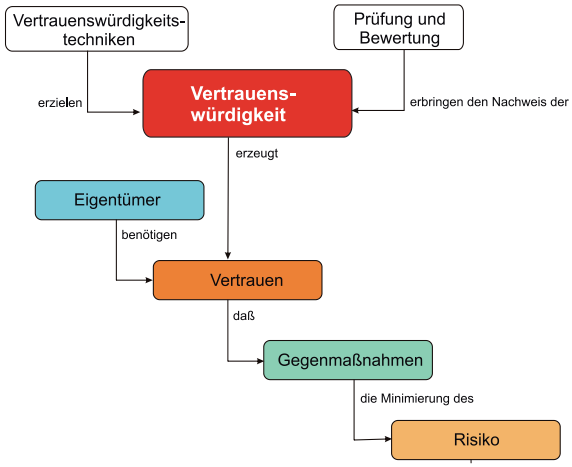

Abbildung 2: Vertrauenswürdigkeitskonzept gemäß den Common Criteria (Quelle: BSI 2006)

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

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

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