nestor
Kompetenznetzwerk Langzeitarchivierung

nestor Handbuch:

Eine kleine Enzyklopädie der digitalen Langzeitarchivierung

8.1 Grundkonzepte der Sicherheit und Vertrauenswürdigkeit digitaler Objekte

Herausgeber:

Heike Neuroth
Hans Liegmann †
Achim Oßwald
Regine Scheffel
Mathias Jehn
Stefan Strathmann

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Im Auftrag von:

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:

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Dr. Heike Neuroth
Forschung und Entwicklung
Papendiek 14
37073 Göttingen
neuroth@sub.uni-goettingen.de
Tel. +49 (0) 55 1 39 38 66

8.1 Grundkonzepte der Sicherheit und Vertrauenswürdigkeit digitaler Objekte

Susanne Dobratz, Astrid Schoger und Niels Fromm

Bezogen auf das Ziel der digitalen Archivierung, die spätere Benutzbarkeit der Objekte zu erhalten und die Informationen zu sichern, finden im Laufe des Lebenszyklus eines digitalen Objektes verschiedene Methoden und Vorgehensweisen Anwendung. Diese werden heutzutage grob als Emulation und Migration bezeichnet. Durch die Anwendung dieser Methoden selbst, aber auch allein durch die Tatsache, dass die digitalen Objekte in einem Archivierungssystem verwaltet werden, sind sie spezielle Bedrohungen ausgesetzt.
Diese Bedrohungen können zum Beispiel sein, vgl. BSI, DRAMBORA, UNESCO, S. 31:

- Höhere Gewalt, wie etwa der Ausfall des IT-Systems, unzulässige Temperatur und Luftfeuchte, etc.;
- Organisatorische Mängel, wie Unerlaubte Ausübung von Rechten, Unzureichende Dokumentation von Archivzugriffen, Fehlerhafte Planung des Aufstellungsortes von Speicher- und Archivsystemen
- Menschliche Fehlhandlungen, wie Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer, Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von Archivsystemen
- Technisches Versagen, wie Defekte Datenträger , Datenverlust bei erschöpftem Speichermedium, Verlust der Datenbankintegrität/-konsistenz , Ausfall oder Störung von Netzkomponenten, fehlerhafte Synchronisierung von Indexdaten bei der Archivierung, Veralten von Kryptoverfahren
- Vorsätzliche Handlungen, wie Manipulation an Daten oder Software, Anschlag, Unberechtigtes Kopieren der Datenträger, Sabotage, Unberechtigtes Überschreiben oder Löschen von Archivmedien

Ein Konzept zur Sicherung der Vertrauenswürdigkeit digitaler Objekte geht immer von der Annahme aus, dass die digitalen Objekte bestimmten Bedrohungen ausgesetzt sind und diese ein Risiko für die digitalen Objekte darstellen, dass es zu minimieren gilt, vgl. BSI 2005.

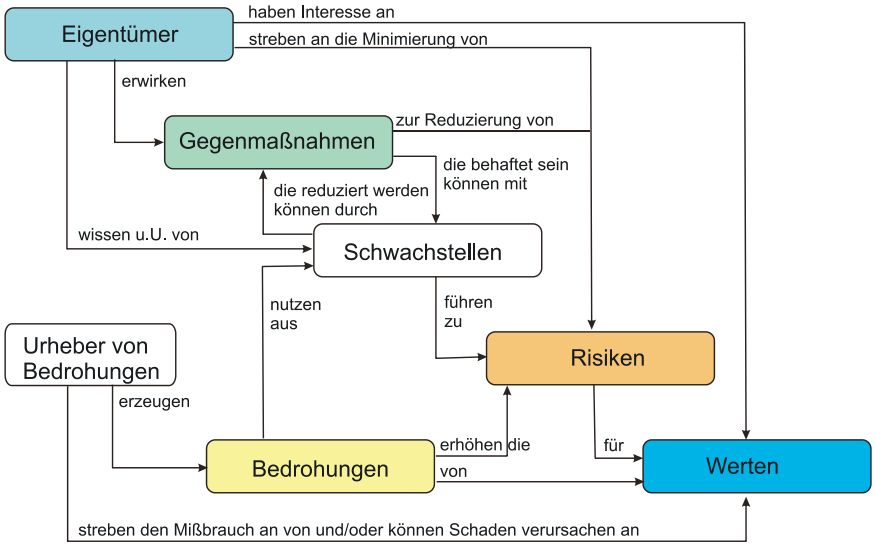

Abb. 8.1.1: Vertrauenswürdigkeitskonzeptgemäß den Common Criteria – Tafel 1

In der IT-Sicherheit, vgl. Steinmetz 2000 geht man davon aus, dass insbesondere folgende Eigenschaften eines digitalen Objektes bedroht sind und man zu deren Schutz entsprechende Maßnahmen ergreifen muss:

1. **Integrität**: bezeichnet den Aspekt, dass die digitalen Objekte unverändert vorliegen
2. **Authentizität**: bezieht sich auf den Aspekt der Nachweisbarkeit der Identität des Erstellers (Urhebers, Autors) und auf die Echtheit der digitalen Objekte
3. **Vertraulichkeit**: bezieht sich darauf, dass unberechtigten Dritten kein Zugang zu den digitalen Objekten gewährleistet wird.
4. **Verfügbarkeit**: bezieht sich auf den Aspekt der Zugänglichkeit zum digitalen Objekt unter Berücksichtigung der Zugriffsrechte
5. **Nichtabstreitbarkeit**: bezeichnet den Aspekt der Prüfung der Authentizität und Integrität digitaler Objekte durch berechtigte Dritte, sodass die Verbindlichkeit der Kommunikation gewährleistet wird, man nennt dies auch Authentifizierung.

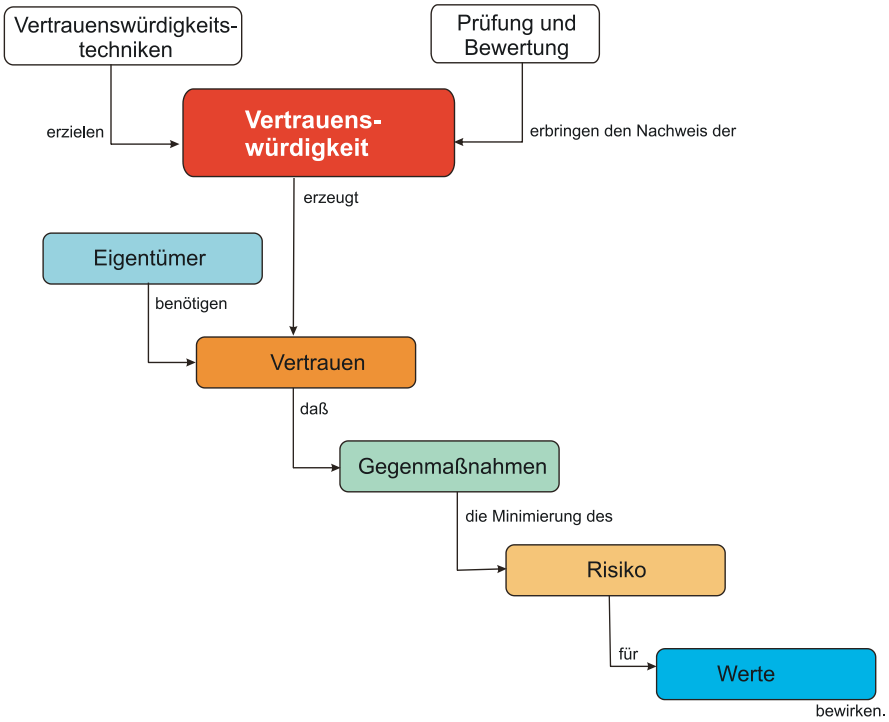

Abb. 8.1.2: Vertrauenswürdigkeitskonzeptgemäß den Common Criteria – Tafel 2

Digitale Langzeitarchive haben den Erhalt der Informationen über lange Zeiträume hinweg zum Ziel. Deshalb ergreifen sie sowohl organisatorische als auch technische Maßnahmen, um diesen Bedrohungen entgegenzuwirken.

Für die Sicherstellung der langfristigen Interpretierbarkeit, trotz der genannten Bedrohungen, ist die Integrität der archivierten digitalen Objekte von großer Bedeutung, da bei der Darstellung dieser Informationen schon wenige fehlerhafte Bits die gesamte Information unlesbar machen können. Zur Überprüfung der Unversehrheit digitaler Objekte, also deren Integrität, werden Hash- und Fingerprinting-Verfahren eingesetzt.
Für die Vertrauenswürdigkeit eines digitalen Langzeitarchivs stellen zudem die Authentizität und die Nichtabstreitbarkeit besonders wichtige Merkmale dar. Dies kann durch eine digitale Signatur der archivierten Objekte erreicht werden. Diese werden im nachfolgenden Kapitel dargestellt.