SLUB
Wir führen Wissen.

Umgang mit Schadsoftware im SLUBArchiv.digital

SLUB Dresden

Version 1.0, 2024-07-30

Inhaltsverzeichnis

Überblick 1
Ingest Prozess 1
Access Prozess 3
Systembetrieb 3
Spezialfall digitale Vor- und Nachlässe 3

Release Note 1.0 vom 2024-07-30

- Erstfassung

Überblick

Dieses Dokument beschreibt den Umgang mit Schadsoftware im SLUBArchiv.digital.

Dieses Dokument ist ein Teil der Übernahmespezifikation für das SLUBArchiv. Zur Übernahmespezifikation gehören die folgenden Dokumente [1]:

- In der **Übernahmevereinbarung** zwischen SLUB und Dienstnehmer sind die Daten, Ansprechpartner und organisatorischen Randbedingungen beschrieben. Dies schliesst die zu verwendenden Handreichungen für Dateiformate bzw. Objektgruppen mit ein.
- In der **Langzeitarchivfähige Dateiformate** sind die Formate aufgeführt, die die SLUB als potenziell archivfähig bewertet und für die die Funktionalitäten der Formaterkennung, Formatvalidierung und Metadatenextraktion in einem ausreichenden Maß durch das SLUBArchiv gewährleistet werden könnten. Die genaue Festlegung erfolgt spezifisch für jeden Workflow und jede Objektgruppe auf Basis der ermittelten signifikanten Eigenschaften.
- Die **SIP Spezifikation für automatischen Ingest SLUBArchiv** beschreibt den Aufbau der Ablieferungspakete (englisch: Submission Information Package, SIP) mit denen der Dienstnehmer die zu archivierenden Dokumente für das SLUBArchiv bereitstellt.
- Die **DIP Spezifikation für automatischen Access SLUBArchiv** beschreibt den Aufbau eines Auslieferungspaketes (englisch: Dissemination Information Package, DIP), welches für die automatische Weiterverarbeitung zielgruppengerechter Ausspielungen (Access) von im SLUBArchiv archivierter digitaler Datenobjekte (IE) geeignet ist
- Die **Workflow Spezifikation für automatisierte Interaktionen mit dem SLUBArchiv** beschreibt den Prozess der Übergabe zu archivierender Dokumente in das SLUBArchiv (Ingest / AIP Update), das Fehlerprotokoll und den Zugriff auf die archivierten digitaler Objekte (Access).
- Das Dokument **Spezifikation Rechteauszeichnung SLUBArchiv** beschreibt, wie rechtliche Informationen zu einem Datenobjekt kodiert und abgelegt werden müssen.
- Das Dokument **Webservice SLUBArchiv** beschreibt Funktionen, die Dienstnehmer nutzen können, um Informationen über ihre Daten im SLUBArchiv über einen Webservice abzufragen.
- Vom SLUBArchiv verwendete Begriffe sind im **Glossar SLUBArchiv** definiert.

Ingest Prozess

Das SLUBArchiv.digital verzichtet auf den Einsatz von Virenscannern während des Ingest-Prozesses innerhalb des Archivinformationssystems.

Üblicherweise wird für den Einsatz von Virenscannern ins Feld geführt, dass diese neben Viren und anderen Schadprogrammen auch nach ausnutzbaren Schwachstellen (z. B. Phishing Signaturen oder CVEs [2]) suchen.

Dateien, denen

- während der Formaterkennung kein Dateiformat zuortenbar, oder
- für die kein Formatvalidator bekannt ist,

können durch Virenscanner geprüft werden.

Aus Sicht des SLUBArchiv.digital sind diese Argumente aber **nicht stichhaltig genug**, um den generellen Einsatz von Virenscannern als Teil des Ingests zu rechtfertigen.

Das SLUBArchiv.digital nimmt nur langzeitarchivwürdige Objekte auf, deren Objekttyp durch eine Handreichung hinreichend spezifiziert und durch eine Übernahmevereinbarung geregelt ist. Für jedes archivfähige Dateiformat, welches diesen Objekttypen zugeordnet ist, ist ein Validator eingerichtet, der Dateien auf ihre Konformität überprüft.

Spezialisierte Dateiformatvalidatoren können Probleme und Abweichungen in Dateien besser und eher entdecken, als generisch arbeitende, signatur-basierte Virenscanner, denen nur bestimmte Byte-Muster bekannt sind.

Das SLUBArchiv.digital vermeidet den Einsatz von digitalen Objekten, die aktive Bestandteile verwenden. Unter "Aktive Bestandteile" versteht man Dateiformat-Bestandteile, die Merkmale einer Programmiersprache oder Virtuellen Maschine aufweisen, wie beispielsweise Javascript, Flash, Postscript, VBA-Makros, Active-X. Dies reduziert Risiken für SLUBArchiv.digital und dessen Nutzer gleichermassen [3].

Weitere Gründe, die gegen die Nutzung von Virenscannern als Teil des Ingests sprechen können, sind:

- unnötig hoher Ressourcenverbrauch, insbesondere I/O-Last durch vermeidbaren Lesevorgang
- zum Zeitpunkt des Virenscans beim Ingest ist eine bestimmte Virensignatur ggf. noch nicht bekannt, die in den eingelieferten Daten aber bereits vorkommt, der Virenscan beim Ingest bietet daher keine Garantie für Virenfreiheit
- Virenscanner erweitern die Angriffsoberfläche, da
  - sie Dateibestandteile interpretieren, die z. B. für ein normales Anzeigeprogramm irrelevant sind
  - von Malware-Erstellern gezielt als Angriffsziel ausgesucht werden
  - sie deutlich komplexer sind
- fälschlich als virenbehaftet markierte Dateien (false-positives) verursachen zusätzliche TA-Arbeit
- höherer Integrationsaufwand, um Virenprüfung im Archivinformationssystem zu ermöglichen
- höherer Administrationsaufwand, da Randbedingungen des Scanners im Einsatz (z. B. maximale Scangrößen, Parallelisierbarkeit) beachtet werden müssen
- im Falle von Vor- und Nachlässen müssen Abbilddateien von Festplatten, Disketten und anderen Datenträgern unverändert übernommen und dürfen nicht in Quarantäne verschoben oder gelöscht werden

Hinweis zu Übernahmevereinbarung / Produzenten

> Mit dem Produzenten sollte vereinbart werden, dass seine Systeme, die Transferpakete bereitstellen, dem BSI-Grundschutz entsprechen.

Access Prozess

Aus ähnlichen Gründen, wie im Ingest Prozess, wird bei der Erstellung der Auslieferungspakete kein Virenscan durchgeführt.

Hinweis zu Übernahmevereinbarung / Konsumenten

Der Konsument ist zu informieren, dass in bestimmten Fällen (siehe Spezialfall digitale Vor- und Nachlässe) eine besonders gesicherte Abspielumgebung eingesetzt werden sollte.

Systembetrieb

Der Systembetrieb des SLUBArchiv.digital folgt den Grundsätzen BSI Grundschutz [https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html]. Die Schnittstellen zum Archiv sind restriktiv gestaltet, sodass die Verbreitung von Schadsoftware weitgehend vermieden wird.

Spezialfall digitale Vor- und Nachlässe

Digitale Vor- und Nachlässe können Abbilddateien von Festplatten, Disketten oder anderen Datenträgern enthalten. Für das Erzeugen dieser Abbilddateien, wie auch für das Arbeiten mit diesen Abbilddateien gelten besondere Anforderungen an den Arbeitsplatz:

- Die Arbeiten erfolgen durch besonders geschultes Personal.
- Der Zugriff auf Schnittstellen, über die externe Hardware angesprochen werden soll, erfolgt hardwaregestützt durch Protokollfilter (z. B. USB-Blocker).
- Der Arbeitsplatz ist nur für den minimal notwendigen Zeitraum einer Übertragung der Inhalte für den Zugriff auf das Intranet freizuschalten.
- Der Arbeitsplatz ist nach BSI Grundschutz [https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html] ausgestattet und aktuell.

[1] Die genannten Dokumente sind auf der Webseite des SLUBArchivs unter https://slubarchiv.slub-dresden.de/technische-standards-fuer-die-ablieferung-von-digitalen-dokumenten/ veröffentlicht und sind dort, technisch bedingt, spezifischer benannt.
[2] Cybersecurity Vulnerabilities (CVE) [https://www.cve.org/About/Overview]
[3] siehe auch Sicherheitsmaßnahmen beim Einsatz aktiver Inhalte [https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_120.html] und BSI Grundschutzkompendium, APP.1.1 Office-Produkte [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/06_APP_Anwendungen/APP_1_1_Office_Produkte_Edition_2023.pdf]