ARCHIVISCHES IT-RISIKOMANAGEMENT

Transferarbeit (55. Wissenschaftlicher Lehrgang an der Archivschule Marburg)

Vorgelegt von:
Stefan Bröhl M.A.
Archivreferendar - Landesarchiv Baden-Württemberg

Gutachter für das Landesarchiv Baden-Württemberg: Dr. Kai Naumann
Gutachter für die Archivschule Marburg: Dr. Burkhard Nolte

Inhaltsverzeichnis

I. Einleitung

Die archivischen Fachaufgaben sind grundlegend vom digitalen Wandel geprägt. Neben den weiterhin bestehenden Anforderungen an eine analoge Bestandserhaltung gilt es zunehmend, digitale Archivalien dauerhaft zu bewahren, die besondere Anforderungen hinsichtlich der Integrität, Authentizität, Vollständigkeit, Zugänglichkeit und Lesbarkeit der Daten haben.[1] Als bündelnder Kernbegriff der jüngeren Debatte, der das Spektrum strategischer Entscheidungen zur Sicherstellung o.g. Parameter von zu archivierenden Daten umfasst, mag die Vertrauenswürdigkeit (*Trust*/*Trustworthiness*) gelten.[2] Vertrauenswürdigkeit und Datensicherheit gehen dabei Hand in Hand. Auf dem Konzept der Vertrauenswürdigkeit basierende Kriterienkataloge zur Konzeption von digitalen Langzeitarchiven empfehlen, Risiken auf organisatorischer, struktureller, rechtlicher und technischer Ebene zu erfassen, abzuwägen und eine angemessene Reaktion zu finden; sprich: Risikomanagement zu betreiben.[3] Im Bereich der analogen archivischen Bestandserhaltung kann die Beschäftigung mit Risiken, eng verknüpft mit dem Krisenbegriff, der Resilienz und Notfallvorsorge, eine längere Tradition und zahlreiche Publikationen vorweisen.[4] Bei der digitalen Archivierung war das Thema Sicherheit freilich auf unterschiedlichen Ebenen und mit variierender Intensität seit jeher mitgedacht, Untersuchungen mit einer Fokussierung auf dem Konzept des Risikos finden sich aber merklich rarer gesät.[5]

---

[1] „Herausforderungen für die Langzeitarchivierung stellen, neben den allgemeinen Sicherheitsbedrohungen unter dem Aspekt der Langfristigkeit, besonders die nicht beständige Bindung der Information an die Datenträger, die physische Alterung der Datenträger sowie die rapiden Veränderungen der für die Interpretation der Repräsentationen erforderlichen technischen Infrastruktur dar. Deshalb werden von den digitalen Langzeitarchiven sowohl organisatorische als auch technische Maßnahmen ergriffen, um die Risiken für den Informationsinhalt zu minimieren …“ (DIN 31644:2012-4, zitiert nach KEITEL/SCHOGER, DIN 31644, S. 78). Vgl. auch: BARATEIRO, Designing, S. 7 f.; KORTE/KUSBER/SCHWALM, E-Government, passim; NIST, Guide, S. 6 f.; XIE, investigation, S. 69. Das Feld der über IT-Sicherheit hinausreichenden Information Security verwendet klassische Schutzziele der *confidentiality*, *integrity* und *availability*, um Bedrohungslagen zu bewerten. Vgl. KRÓL, Relevanz, S. 121. In der Arbeit wird zur verbesserten Lesbarkeit das generische Maskulin verwendet, womit alle Geschlechter eingeschlossen sind.

[2] „Trust is a foundational concept for digital preservation“ (FRANK, Risk, o.S.). Vgl. auch KEITEL/SCHOGER, DIN 31644, S. 20 ff.; DURANTI, InterPARES, passim.

[3] So bspw. bei CoreTrustSeal namentlich bei den Kriterien R4 und R9. Vgl. KEITEL/SCHOGER, DIN 31644, S. 28. Dazu eingehender Kap. II. 2.

[4] So empfiehlt bspw. die Koordinierungsstelle für die Erhaltung des schriftlichen Kulturguts die Durchführung von Risikoanalysen als Fundament der bestandserhalterischen Notfallvorsorge (KEK, Handlungsempfehlungen, S. 73-75). In Frankreich und den Niederlanden, um nur zwei weitere Beispiele zu nennen, gibt es Handreichungen zu Risikoanalysen in der Bestandserhaltung im Archivwesen (BRUN et al., La Sûreté, S. 33 ff.

[5] Einen Literaturüberblick über Risiko-Assessments bei der digitalen Archivierung gibt FRANK, Risk, o.S. (Kapitel: „Literature review“). Einen Überblick über weitere diesbezügliche Methoden und Kataloge bietet: https://en.wikipedia.org/wiki/Digital_preservation#Specific_tools_and_methodologies.

I. 1. Fragestellung und Zielsetzung

An dieser Stelle sollen einige Sätze zur Zielsetzung und Eingrenzung dieser Transferarbeit stehen. IT-Risiko*management*[6] ist, wie der Name schon impliziert, eine komplexe Führungsaufgabe, die zahlreiche organisatorische, rechtliche und technische Aspekte vereint, die Mitarbeit aller Ebenen erfordert und die sich letztlich auf alle Geschäftsprozesse auswirkt.[7] Es kann nicht en passant betrieben werden, wie ein Blick auf die Seitenzahlen der einschlägigen Standards, Handbücher und der jährlich in kaum überschaubarem Maße steigenden Menge an Ratgeberliteratur zeigt.[8] Ziel dieser Arbeit kann es daher nicht sein, umfassende konkrete Risikoanalysen oder gar Handlungsimperative für ein Archiv zu geben. Angesichts der verschiedenartigen strukturellen und organisatorischen Voraussetzungen, Prozesse und Anforderungen der Archive wäre ein solcher Blick von außen von vornerein zum Scheitern verurteilt. Bedingt ist ein solcher Zuschnitt auch durch die quantitative „Quellenlage". Risikomanagement hat immer die Zukunft im Blick, um Bedrohungslagen zu evaluieren und unter dem Blick der Wirtschaftlichkeit auf diese zu reagieren. Im optimalen Fall kann man hierbei auch auf quantitative Daten, also z.B. auf Kennzahlen vergangener Vorfälle zurückgreifen. Da Fragen zur IT-Sicherheit und potenziellen wie tatsächlichen Gefährdungslagen vertraulich behandelt werden, ist ein Blick von außen bisweilen schwer möglich. Mehrere Anfragen des Verfassers an digital archivierende Institutionen wurden mit Verweisen auf die Geheimhaltung von vornerein abschlägig beschieden oder es wurde auf Grundsätzliches verwiesen („Wir halten uns an die einschlägigen Standards ISO etc."). Bei anderen Archiven standen Rücksprachen mit den zuständigen Rechts- und IT-Abteilungen an, die eine Auswertung im Zeitrahmen der Arbeit verhindert haben. Eine quantitative und einigermaßen repräsentative Datenbasis anhand von Fragebögen konnte für eine Auswertung nicht generiert werden. Ziel dieser Arbeit ist es daher:

I.) Ansätze und Methoden von IT-Risikoanalysen anhand der Literatur vorzustellen und einige diesbezügliche Parameter für den archivischen Bereich zu prüfen

II.) durch Expertenbefragungen in Form von Interviews bereits geschehene oder potenzielle Gefährdungen und ihre Folgen zu erörtern.

---

[6] Einen Überblick über den Forschungsstand und verschiedene Methoden der Beschäftigung mit den Themenkomplexen bietet KFN, Cyberangriffe, S. 21-25. Zur thematischen Abgrenzung und den Begrifflichkeiten vgl. BSI-Standard 200-2, S. 14.

[7] NIST, Risk Management Framework, S. 6 f.

[8] KLIPPER, Risk Management, S. 3

I. 2. Öffentliche Einrichtungen, Archive und IT-Sicherheit – Versuch eines Sachstandes

Angriffe auf IT-Strukturen in Unternehmen und öffentlichen Institutionen zeigen seit Jahren eine deutlich steigende Tendenz und Komplexität, Cyberkriminalität ist ein globales und alltägliches Phänomen.[9] Der Jahresbericht des Bundesamtes für Sicherheit in der Informationstechnik nennt die IT-Sicherheitslage für den Untersuchungszeitraum 2021/21 "angespannt bis kritisch" und listet eine Vielzahl an Gefährdungssituationen für staatliche wie nichtstaatliche Institutionen und Akteure auf. Unter den Top-Risiken, auf die sich Unternehmen und Behörden am schlechtesten vorbereitet sehen, finden sich seit Jahren durchgängig Cyberrisiken an erster Stelle.[10]

Grundlegend gilt, dass der überwiegende Teil der Cyberangriffe wirtschaftlich motiviert ist, und größere Unternehmen häufiger betroffen sind als kleine.[11] Cyberangriffe auf kommunale Verwaltungen, Stadtwerke, Gerichte, Universitäten und Forschungseinrichtungen zeigen indes, dass „heute alle Unternehmen, öffentlichen Einrichtungen und Organisation, unabhängig von Bekanntheit, Größe oder Branche, permanent und vollautomatisch auf mögliche Schwachstellen und Einstiegstore gescannt“ werden und potenzielle Ziele von Cyberkriminalität darstellen.[12] Ein Verweis darauf, dass Kultureinrichtungen wie Archive wegen mangelnder Bekanntheit, geringer Größe oder wirtschaftlicher Irrelevanz per se wenig exponiert gegenüber Cyberattacken seien, kann heutzutage nicht mehr gelten:

> „Für Angreifer:innen sind Verwaltung und öffentliche Einrichtungen (…) ein attraktives Ziel. Zwar sind sie in der Regel weniger finanzkräftig als Unternehmen – doch die sensiblen Daten der Bürger:innen machen sie erpressbar.“[13]

Im Jahr 2021 wurde in Deutschland das erste Mal der Cyber-Katastrophenfall ausgerufen,

---

[9] DINIS, Bedeutung, S. 11; KFN, Cyberangriffe, S. 26 f.

[10] GLEIßNER, Grundlagen, S. 101; Allianz Risk Barometer (https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html); BRECHTKEN et al., Identifikation, S. 67; https://www.tagesschau.de/wirtschaft/unternehmen/cyberattacken-unternehmen-risiken-101.html

[11] DINIS, Bedeutung, S. 12; KFN, Cyberangriffe, S. 30 f.

[12] BKA, Cybercrime, S. 6; BSI, Lage, S. 15; Zitat nach BRECHTKEN et. al, Identifikation, S. 74. Im Jahr 2021 ist es u.a. zu substanziellen Cyberangriffen auf die Stadtwerke Pirna, Schwerin und Wismar sowie auf Server der Universitäten Gießen, Köln, der Technischen Universität Nürnberg und der TU Berlin gekommen (https://www.faz.net/aktuell/karriere-hochschule/immer-mehr-hackerangriffe-auf-forschung-und-universitaeten-16802500.html; https://www.deutschlandfunk.de/datenschutz-cyberangriff-auf-das-berliner-kammergericht-100.html). Ähnliche Einschätzungen finden sich bei DONALDSON/BELL, Security, S. 1: „(...) the threat of cyber-attack pervades nearly every type of industry and institution on the Internet“ und WEINREICH, Lean Digitization, S. 127: „Wer ein digitales System oder ein digitales Geschäftsmodell betreibt, kann sicher sein, irgendwann Ziel eines Angriffs zu werden. Leider schützt es auch nicht, klein und unbedeutend zu sein“.

[13] https://taz.de/Cyber-Erpressungen-nehmen-zu/!5837971/

nachdem die Verwaltung des Landkreises Anhalt-Bitterfeld Ziel einer Ransomware-Attacke geworden war.[14] Die Auswirkungen des Angriffs waren noch Monate später zu spüren, an Kosten wird ein mehrstelliger Millionenbetrag erwartet.[15] Als jüngste Entwicklungen mögen die Ereignisse des russisch-ukrainischen Krieges vor Augen geführt werden. Die Mobilisierung von nicht-staatlichen Akteuren und Hackern hat zu einer stark erhöhten Zahl von Cyberangriffen auf Behördenwebseiten und -Datenbanken geführt.[16] Dabei ist es zur Erbeutung und Offenlegung von Datenbanken mit großen Mengen an personenbezogenen Daten gekommen. Wenn Archive und mit ihnen verwandte Kultureinrichtungen bislang eher weniger im Fokus von IT-Sicherheitsanalysen gestanden haben, dürfte es nur eine Frage der Zeit sein, bis ein spektakulärer Präzedenzfall auch im Bereich der öffentlichen Archive eintritt. Da Archive ein integraler Bestandteil der öffentlichen Verwaltung sind und an weiterreichende IT-Strukturen, beispielsweise einer Kommune, angebunden sind, können sie freilich auch von den Folgen eines Cyberangriffs betroffen sein, ohne das hauptsächliche Ziel dargestellt zu haben.[17]

Im englischsprachigen Raum wird die Cybersicherheit im Kontext des Archivwesens in jüngerer Zeit mit großer Vehemenz und Wirkung debattiert und eine Intensivierung der Forschung gefordert.[18] So wurden in Zusätzen zu einer 2019 begonnen Studie über die *National Archives of Australia* (NAA) dieselben als potentielles Ziel von Cyberangriffen identifiziert und dringender Handlungsbedarf angemahnt.[19] Anne LYONS entwirft in ihrem Bericht Szenarien, in denen *hostile actors* das Gerichtswesen Australiens durch manipulierte Beweismittel zum Stillstand brächten, digitale Besitzurkunden und Zertifikate veränderten und damit Amtsgeschäfte wie

---

14 https://www.faz.net/aktuell/wirtschaft/digitec/erster-cyber-katastrophenfall-in-deutschland-landkreis-liegt-lahm-17431739.html.

15 https://www.mz.de/lokal/koethen/alles-wird-teurer-folgen-des-cyberangriffs-kosten-landkreis-anhalt-bitterfeld-bis-zu-zwei-millionen-3322297.

16 https://gazeta.a42.ru/lenta/news/132786-roskomnadzor-v-rossii-rezko-vozroslo-kolicestvo-kiberatak-na; https://www.dw.com/en/ukraine-russia-face-off-in-cyberwar/av-61089184.

17 Zu den wenigen deutschsprachigen Publikationen über die Auswirkungen von Cyberangriffen auf Archive dürfte bislang Thomas KÜBLERs Bericht im Sammelband „Transformation ins Digitale“ (2015) zu zählen sein. Das Stadtarchiv Dresden hatte monatelang mit den Folgen eines Cyberangriffs im Jahr 2014 auf die Stadtverwaltung zu kämpfen. Dieser zog nicht nur Arbeitszeitverluste nach sich, sondern hatte auch die Überlieferungsbildung durch „Datenzerstörungen im Meldewesen, Veterinärwesen und im Finanzbereich“ beeinflusst (KÜBLER, Erfahrungen, S. 90 f.).

18 DONALDSON/BELL, Security, S. 1 f.

19 Das sogenannte *Tune Review of the National Archives of Australia* mit über 100 Anmerkungen und Einsendungen von Interessenvertretern und Experten: https://www.naa.gov.au/about-us/tune-review. Für den von Anne LYONS verfassten Bericht *Identity of a nation. Protecting the digital evidence of who we are* wurden 20 Einrichtungen aus dem Bereich öffentlicher Behörden, Hochschuleinrichtungen und Unternehmen befragt sowie über 70 Experteninterviews, Gesprächskreise und Workshops durchgeführt (LYONS, Identity). Vgl. auch: https://www.smh.com.au/politics/federal/archives-at-risk-of-cyber-attack-security-expert-warns-20210628-p584ts.html.

Immobilienkäufe oder Heiraten verunmöglichten oder durch mutwillige Angriffe auf historische Archive staatliches Handlungsversagen vorführten und öffentliche Entrüstung hervorriefen.[20] Der Staat könne digitale Verluste im 21. Jahrhundert nicht einfach ausgleichen: *Hard paper copies of many key documents simply dont exist*.[21] Als wesentliche Konsequenzen solcher Angriffe betonte LYON, dass das Selbstverständnis der Archive als Träger des kulturellen Gedächtnisses und Bewahrer authentischer Rechtsdokumente wesentlich erschüttert würde und pars pro toto, auch ein grundlegender Vertrauensverlust in die staatlichen Institutionen die Folge wäre. Zwar verfügten die NAA zwar schon über ausgefertigte Pläne hinsichtlich ihrer Cyberresilienz, doch standen bislang unzureichende Mittel im Weg, diese effektiv zu implementieren. David IRVINE betonte, dass öffentliche Archive und ihr Archivgut als Teile kritischer Infrastruktur verstanden werden sollten, die in besonderem Maße von den Auswirkungen von Cyberangriffen betroffen werden könnten.[22] Der Wahrnehmung von Teilen der Politik, dass in Archiven nur alte und irrelevante Sachen verwahrt würden, konnte durch die Untersuchungsberichte jedenfalls abgeholfen werden: Mitte 2021 bekamen die *National Archives of Australia* einen Sonderetat von 67.7 Mio. AU$ zur Umsetzung von Digitalisierungsstrategien zur Verfügung gestellt, worin der Verbesserung der IT-Sicherheit nunmehr explizit größte Priorität eingeräumt wurde.[23] Auch in anderen Ländern wurde in den letzten Jahren die Verbesserung der Cybersicherheit staatlicher Institutionen aufgrund der Zunahme von Cyberattacken auf Behörden zur Chefsache erklärt und massive finanzielle wie strukturelle Veränderungen vorgenommen.[24] Trotz

[20] „A synchronised attack on half a dozen key historical archives—such as our entire newspaper archives, historical photo databases, war records and Indigenous archives—would cause an irreplaceable loss that would be likely to cause public outrage and a great collective sense of loss.“ Das *Digital Preservation Handbook* der *Digital Preservation Coalition* listet ähnliche und weitere Konsequenzen von Datenverlusten auf (https://www.dpconline.org/handbook/institutional-strategies/risk-and-change-management).

[21] Vergleiche auch die Aussage des estnischen Sicherheitsbeamten (englische Bezeichnung: *Government CIO of Estonia*) Siim SIKKUT: „If we lose digital records, we are done as a country. We don't keep paper backups.“ Das im Bereich der öffentlichen digitalen Verwaltung vergleichsweise fortschrittliche Estland hat in Luxemburg zwischen 2015 und 2017 eine sog. Daten-Botschaft, mit Backups wichtiger personenbezogener Daten der Landesbewohner, anlegen lassen (https://euobserver.com/digital/138406; https://e-estonia.com/estonia-to-open-the-worlds-first-data-embassy-in-luxembourg/).

[22] „Government archive material, must be considered as equivalent to any critical national infrastructure, given its value to national identity, values, history. Critical infrastructure is firmly in the sights of those conducting cyberwarfare and industrial sabotage“ (LYONS, Identity). Ein formuliertes Ziel des Strategiepapieres war es, *national identity assets* als Gefüge der kritischen Infrastruktur zu verstehen.

[23] https://www.itnews.com.au/news/national-archives-gets-67m-to-digitise-records-boost-cyber-security-566785. Vgl. auch: TUNE, Review, S. 48 ff.

[24] In Frankreich wird eine Summe von 1 Mrd. € bis zum Jahr 2025 für ein Maßnahmenpaket veranschlagt (https://www.20minutes.fr/high-tech/2979367-20210217-cyberattaques-elysee-promet-1-milliard-euros-contrer-menace-croissante). Vgl. auch FUZEAU, Records Management, S. 131 f. In Norwegen befindet sich in dem Maßnahmenkatalog zu einer 2019 initiierten Nationalen Cybersicherheitsstrategie u.a. ein IT-Risikomanagement-Tool für Unternehmen und Behörden unter dem Namen *Comprehensive Cyber Security Risk Assessment* in Entwicklung. Siehe: https://www.regjeringen.no/en/dokumenter/national-cyber-

dieser erfreulichen Etat-Aufstockungen zeigt sich indes, dass ein Mangel an IT-Personal auch im Archivwesen die Implementierung von IT-Sicherheitsstrategien erschweren kann.[25]

Es lassen sich, in Anlehnung an LYONS, weitere fiktive Szenarien entwerfen, die den Konnex IT-Sicherheit-Archiv verdeutlichen:

> Szenario 1: Die IT-Systeme einer städtischen Verwaltung werden von einem Ransomware-Angriff betroffen. Die Verwaltung reagiert mit der Ablehnung der Geldforderung, dem weitgehenden Herunterfahren der IT-Infrastruktur und der schrittweisen Reaktivierung von Backups. Das kommunale Archiv steht in der Prioritätenliste weit unten, noch nach Monaten ist der Zugriff auf wichtige Software wie archivische Fachinformationssysteme nicht möglich. Die Erledigung aller archivischen Fachaufgaben ist betroffen. In Folge der sukzessiven Öffnung der Kommunikationswege in der Verwaltung entsteht eine hybride Schriftgutverwaltung, die die künftige Überlieferungsbildung im Archiv prägen wird, zumal der Datenverlust digitaler Assets (z.B. der archivierten städtischen Webseiten sowie der von Bürgern eingereichten Datensätze der Aktion: „Unsere Stadt in Zeiten der Pandemie!“) immer noch immer nicht einzuschätzen ist.
>
> Szenario 2: In einem Wirtschaftsarchiv lagern als Deposita Geschäftsunterlagen, die aufgrund geschäftsrelevanter Daten nur nach Antrag und mit Zustimmung der abgebenden Unternehmen eingesehen werden dürfen. Das Archiv hat früh damit begonnen, im Zuge von Digitalisierungsaktionen Teile der Unterlagen in ein digitales Langzeitarchiv zu übernehmen. Aufgrund der geringen Größe des Archivs war ein Mitarbeiter für zentrale Workflows der digitalen Archivierung hauptverantwortlich. Mit Versionierungen und Protokollierungen existieren Kontrollmechanismen innerhalb des digitalen Archivierungssystems, ein vier-Augen-System war aber nicht vorgesehen. Nachdem zwischen der Hausleitung und dem Mitarbeiter wiederholt Konflikte bestanden hatten, kündigt er frustriert seinen Job. Dem Nachfolger fällt auf, dass in den Wochen davor wiederholt umfassende Zugriffe auf Primärdaten geschehen sind.

security-strategy-for-norway/id2627177/ in der *List of measures*, S. 12.

[25] So der Tenor mehrerer Aussagen von Interviewpartnern, vornehmlich aus dem Bereich der staatlichen Archive.

> Szenario 3: In der Öffentlichkeit wird vermehrt über IT-Sicherheitsvorfälle berichtet, die auch deutsche Archive betroffen haben. Aufgrund des professionellen Vorgehens wird eine Mittäterschaft von Nachrichtendiensten im Ausland vermutet. Seitens einer abgebenden Behörde zeigt sich, dass diese zunehmend unwilliger wird, dem Archiv selbst analoge Unterlagen anzubieten, die womöglich einen geheimdienstlichen Methodenschutz unterliegen. Planungen für ein digitales Verschlusssachen-Magazin kommen ins Stocken.

Die Szenarien sind fiktiv, von den gängigen Methoden, Akteuren und Schadensbildern von Risiken der Informationssicherheit dürften Archive wie alle anderen öffentlichen Einrichtungen betroffen sein. Warum ein steuernder Umgang von Risiken, der darüber hinausgehend auch spezifische Herausforderungen von (Langzeit-)Archiven in den Blick nimmt, lohnend sein kann, soll im Folgenden angerissen werden.

II. IT-Risikomanagement – Vorteile und Standards

II. 1. Warum überhaupt Risikomanagement betreiben?

Risikomanagement zielt wesentlich auf die Frage des Ressourceneinsatzes: Welche Kosten ist man bereit, zur Verminderung oder Vermeidung der Folgen erkannter Risiken zu investieren, welche Risiken sind zu tolerieren oder können vernachlässigt werden? In diesem Sinne betreibt jede Institution eine Form des Umgangs mit Risiken, auch wenn ein umfassendes und systematisches Risiko-Management für die meisten Einrichtungen im Bereich der digitalen Archivierung bislang eine Ausnahme darstellen dürfte. Sebastian KLIPPER merkt hierzu an:

> „Sicherheitsentscheidungen kann man nicht aus dem Weg gehen, selbst dann nicht, wenn man sich dagegen wehrt. Selbst das Aufschieben einer Sicherheitsmaßnahme ist eine Entscheidung gegen deren sofortige Umsetzung. In diesem Sinn gibt es auch in jedem Unternehmen und jeder Behörde eine Form von Sicherheitskultur, auch wenn damit weder ein Ziel verfolgt wird, noch nachvollziehbar oder gar messbar wäre, was bisher erreicht wurde und was nicht.“[26]

Eine optimierte Sicherheitsstrategie zielt auf die Vermeidung von Unter- wie auch von Überinvestitionen in die Sicherheit und auf die Erreichung eines balancierten Idealpunktes zwischen den eingesetzten Ressourcen und den aus einer verbesserten Sicherheitslage resultierenden Vorteilen. Der Grundgedanke kann auch Geltung für ein nicht wirtschaftlich arbeitende Einrichtung wie ein Archiv beanspruchen, wie die

[26] KLIPPER, Konfliktmanagement, S. 163 f.

folgenden Grafiken skizzieren sollen:

[Abb. 1 z. Veröff. entfernt]

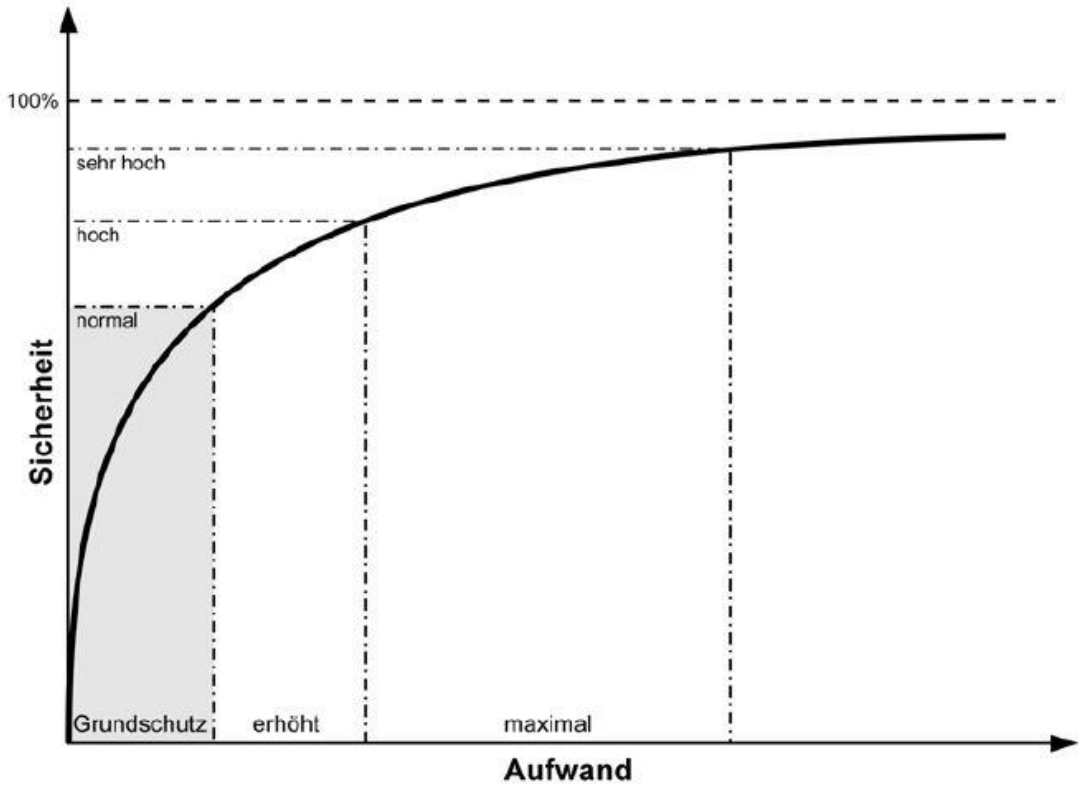

Abb. 1 und 2: Schematische Darstellung des Return of Investment (ROI) in der Informationssicherheit und der Aufwand-Nutzen-Relation nach BSI-Standard 100-2[27]

Risikoanalysen werden im Bereich der analogen Bestandserhaltung von Museen und Archiven (bzw. allen Arten von *collections*) vor allem in der anglophonen Welt seit Jahrzehnten empfohlen und durchgeführt.[28] Für Deutschland mag hier stellvertretend die Empfehlung der Koordinierungsstelle für die Erhaltung des schriftlichen Kulturguts (KEK) gelten, die die Durchführung von Risikoanalysen als Fundament der bestandserhalterischen Notfallvorsorge ansieht.[29] Als Beispiel für die Anwendung von Methoden des Risikomanagements sei die Transferarbeit von Richard LANGE zum Bedrohungsbild Terrorismus genannt.[30] Wenn auf dem Begriff des Risikos fußende Methoden in die strategische Ausrichtung und längerfristige Finanzplanung eines Archives integriert werden, kann von Risiko*management* gesprochen werden, das

[27] Entnommen aus: CALDER/WATKINS, Information Security Risk, Chapter 3; BSI, Standard 100-2, S. 32.
[28] Vgl. BÜLOW, Risk Management, S. 61; RCE, Risk Management.
[29] KEK, Handlungsempfehlungen, S. 73-75.
[30] LANGE, Terror.

Teilaspekte wie die Identifikation, Analyse und schließlich die Bewältigung von Risiken umfasst.

II. 2. Standards, Normen und Empfehlungen

Der Risikobegriff darf in der Diskussion um Vertraulichkeit in der digitalen Archivierung als grundlegendes Konzept angesehen werden, ohne den die Beschäftigung mit dem Thema Datensicherheit nicht auskommt.[31] Kriterienkataloge wie Trustworthy Repositories Audit and Certification (TRAC), das die Grundlage für die spätere ISO 16363 bildet und DRAMBORA (Digital Repository Audit Method Based On Risk Assessment) betonen die Bedeutung von kontinuierlichen Risiko-Assessments in den sich stetig wandelnden technischen und strukturellen Umgebungen von Langzeitarchiven.[32] Die DIN 31644 bildet für den deutschsprachigen Raum den jüngeren Kulminationspunkt einer jahrelangen internationalen Debatte um die Vertrauenswürdigkeit digitaler Archive; ein von Christian KEITEL und Astrid SCHOGER herausgegebener Kommentar (2013) liegt vor.[33] Im Kriterium K34 der Norm werden Schritte zur Entwicklung eines Sicherheitskonzeptes gefordert, das u.a. die „Bestimmung des zu schützenden Objektes und der Schutzziele, Analyse der Bedrohungen/Schadensszenarien/Gefahren, Bewertung von Eintrittswahrscheinlichkeit und potentieller Schadensschwere, Entwicklung von Maßnahmen zur Reduzierung der Eintrittswahrscheinlichkeit und Schadenshöhe, Planung von Maßnahmen und Bereitstellung von Mitteln zur Schadensbekämpfung und -eindämmung, wenn das Risiko schlagend wird“ beinhaltet – womit die wesentlichen Schritte des Risikomanagements umrissen sind.[34] Ein Unterschied sollte dabei zwischen vorsätzlichen und fahrlässigen Handlungen bzw. menschlichem und technischem Versagen gemacht werden. Das die DIN 31644 referenzierende *nestor Siegel für vertrauenswürdige digitale Langzeitarchive* sieht zu Kriterium K34 explizit eine „Analyse des archivspezifischen Bedrohungspotentials“ vor, um darauf aufbauend, ein Gesamtsicherheitskonzept für die Organisation zu bilden.[35]

Die aktuellen einschlägigen Normen der Risikoanalyse sind jene der ISO 31000-Reihe, die einen allgemeinen Rahmen für Risikomanagement abbilden sowie die ISO

[31] FRANK, Risk, S. 1, 26; BARATEIRO, Designing, S. 7.
[32] Einen Überblick über die Implementierung der Zertifikate in diversen Institutionen bietet FRANK, Disaster Planning, S. 15 ff.
[33] KEITEL/SCHOGER, DIN 31644.
[34] Vgl. KEITEL/SCHOGER, DIN 31644, S. 69, S. 109.
[35] Hier u.a. mit den Fragen: „Welche böswilligen bzw. auf menschliches oder technisches Versagen zurück gehenden Schadensszenarien erachten Sie als besonders gefährdend für den Erhalt der Informationsobjekte und Repräsentationen? Wie hoch sind die Eintrittswahrscheinlichkeiten der Schadensfälle? Wie hoch ist die Schadensschwere? Welches Restrisiko wird noch akzeptiert?“ (nestor, Erläuterungen, S. 56 f.).

27000er-Reihe, die spezieller im Bereich der Informationssicherheit Geltung beansprucht (hier v.a. die ISO 27001 und 27005).[36] Als einen wichtigen Unterschied betont KLIPPER, dass in der später erschienen ISO 31000 das Risikomanagement positiv als „Garant für Wertzuwachs“ verstanden wird, während bei der ISO 27005 quasi nur Schäden und keine Gewinne erzielt werden.[37] Dieser Unterschied sollte bei der Kommunikation gegenüber dem Geldgeber bedacht werden, um den Eindruck zu vermeiden, dass Sicherheit nur Geld koste (Stichwort: Return on Investment, ROI).

Die Sicherstellung der Vertrauenswürdigkeit und einen systematischen Umgang mit diesbezüglichen Risiken darf man als einen wesentlichen Beitrag zur archivischen Kernaufgabe der Bestandserhaltung und letztlich auch der Nutzung verstehen. Beispielhafte Ziele der Informationssicherheit, wie sie das Bundesamt für Sicherheit in der Informationstechnik formuliert – darunter die „hohe Verlässlichkeit des Handelns, auch in Bezug auf den Umgang mit Informationen (Verfügbarkeit, Integrität, Vertraulichkeit)“, die „Gewährleistung der guten Reputation der Institution in der Öffentlichkeit“, die „Sicherung der hohen, möglicherweise unwiederbringlichen Werte der verarbeiteten Informationen“ sowie die „Gewährleistung der aus gesetzlichen Vorgaben resultierenden Anforderungen“ – lassen sich auch leicht erkennbar auf die ethischen wie rechtlichen Maßstäbe und Vorgaben des archivarischen Handelns beziehen.[38]

Die Nutzbarmachung von Begriffen und Methoden des Risikomanagements zur Evaluierung und Verbesserung der Informationssicherheit dürfte im Zuge einer tendenziell wachsenden IT-Bedrohungslage und den besonderen Anforderungen an den Schutz personenbezogener Massendaten in digitalen Archiven einen Bedeutungszuwachs in der Zukunft erfahren. Hier sei zuletzt an die Thematik von digitalen Verschlusssachen-Magazinen gedacht, bei deren Etablierung dem Aspekt der Sicherheit – und damit auch des Risikos - in besonderen Maße Rücksicht gezollt werden muss.[39]

---

[36] BSI, Grundschutz, S. 6; https://www.onlinesicherheit.gv.at/Themen/Experteninformation/Normen-und-Standards/ISO-IEC-27000.html. Einen Überblick über die Normen bietet KLIPPER, Risk Management, S. 23-41.

[37] KLIPPER, Risk Management, S. 29 f. Zitat nach S. 29.

[38] BSI-Standard 200-2, S. 23 f.

[39] So sieht die Digitalstrategie des Hessischen Landesarchivs (2019), S. 16, vor: „Was schon für analoge Unterlagen gilt, bedarf im digitalen Umfeld wegen der vielfältigeren Missbrauchsmöglichkeiten und der weitreichenderen Auswirkungen einer besonderen Beachtung (...) Für besonders sensibles personenbezogenes Archivgut mit hohem Schutzbedarf sind zusätzliche Schutzmaßnahmen umzusetzen – sowohl bei der digitalen Archivierung als auch bei der Recherche von analogem Archivgut (…) Für digitale Daten, die der Geheimhaltung unterliegen (Verschlusssachen), sind gesonderte Konzepte und Strukturen für die digitale Archivierung zu schaffen.“ (https://landesarchiv.hessen.de/sites/landesarchiv.hessen.de/files/digitalstrategie_hla.pdf).

III. Methoden und Vorgehensweise von Risikoanalysen

III. 1. Risikoanalysen: Definition und allgemeines Vorgehen

Als klassische Definition eines Risikos kann ein unsicheres Ereignis verstanden werden, das im Falle des Eintritts negative Auswirkungen hat.[40] Die in ihrer Einfachheit bestechende und vielfach zu findende Lehrbuchformel definiert Risiko als das Produkt von Schaden und Eintrittswahrscheinlichkeit:[41]

Risiko = (Potenzieller) Schaden * Eintrittswahrscheinlichkeit

Eine Gefahr sollte nur dann im Kontext von Risikoanalysen behandelt werden, wenn sie eine realistische Eintrittswahrscheinlichkeit hat. Sebastian KLIPPER hat hinsichtlich der Auflistungen von typischen Bedrohungen im Risikomanagement kritisiert, dass höhere Gewalt und Extremereignisse wie Flugzeugabstürze oder Vulkanausbrüche beliebte und ständig wiederholte Topoi im Risikomanagement seien, und dabei gegenüber dem Risikofaktor Nr. 1 – dem menschlichen Handeln – ein zu großes Gewicht eingeräumt bekämen.[42] Dieser Einschätzung folgen zahlreiche weitere Studien, die betonen, dass unsensibilisierte oder fahrlässig handelnde Mitarbeiter als größte Bedrohungsfaktoren der Informationssicherheit anzusehen sind.[43]

Die Etablierung eines übergreifendes Risikomanagementsystems ist eine zeitaufwendige Führungsaufgabe, die nicht ansatzweise auf ein paar Seiten abgehandelt werden kann. Aus der umfassenden Literatur können daher im Folgenden nur einige Aspekte aufgegriffen werden, die das Nachdenken über Bedrohungslagen für digitale

---

[40] DINIS, Bedeutung, S. 30. Das BSI-Glossar definiert Risiko „als die Kombination (also dem Produkt) aus der Häufigkeit, mit der ein Schaden auftritt und dem Ausmaß dieses Schadens. Der Schaden wird häufig als Differenz zwischen einem geplanten und ungeplanten Ergebnis dargestellt. Risiko ist eine spezielle Form der Unsicherheit oder besser Unwägbarkeit." (BSI, Grundschutz, S. 6). Als Beispiel einer rechtlichen Definition im Sinne der DSGVO gilt Risiko als das „Bestehen der Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden (einschließlich ungerechtfertigter Beeinträchtigung von Rechten und Freiheiten natürlicher Personen) darstellt oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann. Es hat zwei Dimensionen: Erstens die Schwere des Schadens und zweitens die Wahrscheinlichkeit, dass das Ereignis und die Folgeschäden eintreten." (DSK, Risiko). Zu „konstruktivistischen" Definitionen des Risikos und weiteren Literaturhinweisen siehe auch: FRANK, Risk, o.S.

[41] HARICH, IT-Risikomanagement, Kap. 10.8.1. Vgl. im Folgenden auch: BARTELEIT, Risikoanalyse, S. 14 ff.

[42] „[In vielen Aufzählungen von Bedrohungslagen] steht die höhere Gewalt an erster Stelle. Da brennt erst alles nieder, bevor es überflutet wird und anschließend von einem Erdbeben dem Erdboden gleich gemacht wird. Da fallen Flugzeuge vom Himmel, Klimaschwankungen lassen die Server ausfallen und sogar Vulkane brechen aus. Sogar Atomschläge werden aufgeführt, bevor der Blick auf den Menschen fällt" (KLIPPER, Risk Management, S. 45). Vgl. auch KRÓL, Relevanz, S. 173 f.

[43] Ein unsensibilisierter Beschäftigter ist „stets das schwächste Glied der Informationssicherheit" (DINIS, Bedeutung, S. 60). „Insbesondere organisatorische Maßnahmen, die den Faktor Mensch betreffen, scheinen bei der Prävention von Cyberangriffen einen Unterschied zu machen und sind demnach in Hinblick auf ihre Verbreitung vor allem bei kleinen und mittleren Unternehmen besonders zu fördern." (KFN, Cyberangriffe, S. 169).

Archive erleichtern können. Die im Folgenden skizzierte Vorgehensweise beim Risikomanagement basiert auf einer Straffung der in der Literatur üblichen Kernpunkte, auf denen die meisten Risikomanagementverfahren beruhen. Risikomanagement kann etwa in die Phasen der Risikoidentifikation, der Risikoanalyse sowie der Risikobewältigung unterteilt werden.[44] In der Phase der Risikoidentifikation werden bestehende sowie zukünftige bzw. unbekannte Risiken analysiert. Ziel ist es, über bereits bekannte Risiken hinaus weitere potenzielle Gefährdungen durch systematische Verfahren und Kategorisierungen zu erschließen. In der auf die Identifikation aufbauenden Risikoanalyse werden die erkannten Risiken quantifiziert, d.h. auf Eintrittswahrscheinlichkeit und Schadenshöhe bewertet. Für die Datenlage quantitativer Analysen gilt, dass diese häufig unzureichend ist oder Werte sich nicht festlegen lassen. Die Verwendung von konkreten Schadensfallzahlen vergangener Vorfälle muss im Hinblick auf die Verwendung zukünftiger Prognosen mit Vorsicht geschehen, da Bedrohungslagen hinsichtlich ihrer Intensität und Häufigkeit im stetigen Wandel inbegriffen sind.[45] Wo keine Kennzahlen vorhanden sind oder diese sich nicht ermitteln lassen, kann eine Risikobewertung durch qualitative Bewertungen, meist 3- oder 5-skalierte Kategorisierung („sehr unwahrscheinlich – sehr wahrscheinlich) erweitert oder substituiert werden. Die Abschätzungen beruhen daher häufig auf Annahmen und Schätzungen.[46] Hinsichtlich der Methoden zur Generierung von Daten bei Risiko-Analysen findet sich bei Klipper (2015) eine komprimierte Auflistung von 12 Methoden nach ISO 31010, die von Brainstorming über Root-Cause-Analysen hin zu Entscheidungsmatrizen reichen.[47] Die Methoden unterscheiden sich hinsichtlich ihrer Vorbereitung, ihres Ressourcenbedarfes und ihres Outputs wesentlich. Die übliche Darstellungsform der erstellten Analysen folgt in einer Risiko-Matrix.[48] Bei der Risikobewältigung bzw. Risikosteuerung wird versucht, eine Risk-Return-Optimierung

[44] Vgl. im Folgenden: DINIS, Bedeutung, S. 14 ff., S. 57 ff.; GLEIßNER, Grundlagen, passim; BBK, Methode, S. 45 ff. Da Risikomanagement als übergreifendes Konzept verstanden wird, kann das Verfahren je nach Anwendungsfeld und Managementphilosophie durch eine Vielzahl weiterer Phasen und Parameter modifiziert werden.

[45] KLIPPER, Risk Management, S. 73.

[46] „Bei der Risikoanalyse ist das richtige Maß an wissenschaftlichem Anspruch und pragmatischem Vorgehen zu finden. Immer dann, wenn keine oder zu wenige statistische/wissenschaftliche Erkenntnisse vorliegen, müssen Wissensdefizite (zunächst) durch begründete Annahmen und Schätzungen kompensiert werden können“ (BBK, Methode, S. 17); „Selbst hervorragend analysierte Risiken sind nicht unerheblich von geschätzten Größen abhängig. Potentielle Schadenshöhen oder Eintrittswahrscheinlichkeiten stehen nicht in irgend einer international anerkannten Tabelle, aus der man nur abzulesen bräuchte. Es handelt sich hierbei um interne oder externe Schätzgrößen oder Erfahrungen der Vergangenheit, zu deren Festlegung man unterschiedlichster Meinung sein kann“ (KLIPPER, Risk Management, S. IX.).

[47] KLIPPER, Risk Management, S. 107 ff.

[48] BBK, Methode, S. 21.

zwischen eingesetzten Kosten und Nutzen bei der Implementierung von Steuerungsstrategien zu erreichen. Ziel ist nicht die grundsätzliche Vermeidung aller Risiken, sondern eine nach strategischen Gründen begründete Steuerung von Risiken. Die Risikobewältigung basiert auf ursachenbezogenen Strategien wie der Vermeidung bzw. der Verminderung der Eintrittswahrscheinlichkeit erkannter Risiken sowie wirkungsbezogenen Maßnahmen wie der Begrenzung der Schadenshöhe im Eintrittsfalle.[49]

Risikoanalysen und -bewertungen werden üblicherweise anhand der Parameter Bedrohungen (*threats*), Schwachstellen (*vulnerabilities*), Geschäftswerte (*assets*) und Schadenswirkungen (*impacts*) vorgenommen, wobei hier je nach Umfang und Zuschnitt unterschiedliche Gewichtungen gesetzt werden können.[50] Der Archivar muss an dieser Stelle nicht das Rad neu erfinden, sondern kann auf bereits etablierte Muster zurückgreifen und darauf aufbauen, z.B. anhand von Methoden und Grundlagen des IT-Grundschutzes oder des Standard-Datenschutzmodells (DSM).

III. 2. Vorgehen nach IT-Grundschutz und ASIT

Der wesentliche Grundgedanke des vom BSI entwickelten IT-Grundschutzes ist, dass mit verhältnismäßig geringem Aufwand ein relativ hohes Schutzniveau gegen gängige Bedrohungen erreicht wird.[51] Die Auswahl von Gefährdungen und Sicherheitsmaßnahmen, die für das jeweilige Zielobjekt relevant sein können, erfolgt nach dem Baukastenprinzip anhand von Katalogen. Der Zeitaufwand wird durch den Verzicht auf aufwendige Detailanalysen stark reduziert, da typische Gefährdungen kreuzreferenzierbar sind. Für jeden Geschäftsprozess bzw. jedes Asset wird zuerst eine Liste mit den relevanten IT-Grundschutz-Gefährdungen zusammengestellt, die von G01 (Feuer) bis G047 (schädliche Seiteneffekte IT-gestützter Angriffe) reichen und mit Beispielen angereichert sind. Diese elementaren Gefährdungen können noch durch

[49] GLEIßNER, Grundlagen, S. 283 ff.
[50] Vgl. im Folgenden: ASIT, Sicherheitshandbuch, S. 116 ff.
[51] BSI Standard 100-2, S. 10. Vgl. auch: ASIT, Sicherheitshandbuch, S. 127 ff.; KLIPPER, Risk Management, S. 161 f. Nach BRYDE/ GONZÁLEZ, die sich auf Befunde der Norwegischen *Nasjonal sikkerhetsmyndighet* (National Security Authority) stützen, kann die Befolgung einer Reihe verhältnismäßig einfach zu implementierender Regeln zu einer wesentlichen Verringerung von internetgestützten Angriffen führen. BRYDE/GONZÁLEZ, Secure Data, S. 336. Dazu gehören: *hardware and software must be state of the art* (1), *update security software as fast as possible* (2), *never distribute administrator rights to end-user* (3), *block any unauthorized programs* (4). BRYDE/GONZÁLEZ geben eine Verringerung von 80-90% von internet-basierten Angriffen an, wobei die Quellengrundlage nicht referenziert wird. Diese und ähnliche Maßnahmen finden sich aber auch in aktuellen BSI-Empfehlungen vom 28.02.2022 angesichts der Bedrohungslage im Zuge der Ukraine-Krise wieder (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Vorfaelle/Ukraine-Krise/Massnahmenempfehlungen_BSI_Ukraine.html?nn=1025778#download=1=). Vgl. im Folgenden auch: KLIPPER, Risk Management, S. 100 ff.

Spezifika des jeweiligen Geschäftsprozesses ergänzt werden. Für Objekte, für die ein normaler Schutzbedarf in den Werten Vertraulichkeit, Integrität und Verfügbarkeit festgestellt wird, gelten die dort empfohlenen Sicherheitsmaßnahmen als ausreichend. Darüber hinaus gibt der Grundschutz aber auch Hilfestellungen, um eine vereinfachte Analyse von solchen Objekten durchzuführen, die einen „hohen oder sehr hohen Schutzbedarf" in einem der drei genannten Parameter haben.[52] Für die Bestimmung des Sicherheitsniveaus von Prozessen und Assets (z.B. Räume, IT-Systeme) bietet das IT-Grundschutz-Kompendium weitere Hilfestellungen zur Bestimmung.[53] Vereinfacht gesagt, sollte eine Risikoanalyse dann stattfinden, wenn die im IT-Grundschutz genannten Maßnahmen nicht als ausreichend angesehen werden. Das Österreichische Informationssicherheitshandbuch unterscheidet drei Strategien zum Vorgehen bei IT-Risikoanalysen:[54]

1. Eine detaillierte Risikoanalyse aller IT-Systeme, die zusammenführende Analysen von allen Assets, Bedrohungen und Schwachstellen vornimmt, aber zeitaufwendig und ressourcenintensiv ist

2. Ein Grundschutzansatz, der für alle Systeme die Implementierung von Grundschutzmaßnahmen vorsieht, aber auf detaillierte Risikoanalysen verzichtet

3. Kombinierter Ansatz: Hierbei wird in einem ersten Schritt für alle einzelnen IT-Systeme der Schutzbedarf ermittelt. Während bei Systemen mit geringem oder mittlere Schutzbedarf Grundschutzmaßnahmen angewandt werden, werden jene mit einem hohen oder sehr hohen festgestelltem Schutzbedarf einer detaillierten Risikoanalyse unterzogen

Der kombinierte Ansatz ist nach den Empfehlungen der ASIT für die meisten Umgebungen empfehlenswert, da er bei gleichbleibendem angemessenen Grundschutz aller Systeme weitergehende, individuelle Sicherheitsmaßnahmen zulässt. Im IT-Grundschutz und dem Vorgehen nach ASIT-Sicherheitshandbuch nehmen Risikoanalysen somit eine zentrale Rolle ein. Der grundlegende Gedanke einer Unterscheidung zwischen grundsätzlichen Maßnahmen und darüberhinausgehenden Assessments von Risiken besonders schutzbedürftiger Assets und Prozesse dürfte auch auf den archivischen Bereich übertragbar sein. Hierin liegt auch das Potential, wie sich der Archivar in den Prozess von Risikoanalysen einbringen kann. Technische Detailfragen zu

[52] BSI-Standard 100-3, S. 4. Vgl. auch KLIPPER, Risk Management, S. 100 ff.
[53] BSI-Standard 200-2, S. 104 ff.
[54] ASIT, Sicherheitshandbuch, S. 115 ff.

Authentifizierungsmöglichkeiten bei einer Softwareanwendung oder der Konfiguration einer Firewall sind wichtig – und tatsächlich Sache der zuständigen IT-Leistungsbringer. Es darf davon ausgegangen werden, dass Gefährdungslagen nach BSI-Grundschutz z.B. grundlegend durchexerziert worden sind und entsprechende Sicherheitsvorkehrungen für die Informationssysteme getroffen wurden. Der Wert der archivischen Assets und damit verknüpft auch der Schadenswirkungen kann indes nur von denjenigen genauer bestimmt werden, die mit den zu archivierenden Daten vertraut sind. Für die Betrachtungen von Sicherheitsrisiken in digitalen Archiven bietet sich vornehmlich eine Klassifizierung der archivspezifischen Assets und ihrer spezifischen Schutzniveaus an.

III. 3. Archivische Assets

Zu den bedrohten Assets können alle für den Betrieb einer Organisation relevanten Objekte zählen, z.B. physische Objekte wie Gebäude und Datenträger, logische Objekte wie Software und Daten, Personen und Fähigkeiten. Theoretisch kann man einen einzelnen Laptop oder eine Datenbank als Assets für Risikoanalysen betrachten, in der Praxis empfiehlt sich aber die Aggregation von ähnlichen Entitäten und die einheitliche Behandlung von diesen. Die britischen Nationalarchive empfehlen die Zusammenstellung relevanter *information assets* einer Organisation als ersten und wichtigen Schritt zur Identifizierung möglicher Risiken bei der digitalen Langzeitarchivierung.[55]

[55] „Als Asset wird alles bezeichnet, was für eine Organisation einen Wert hat“, z.B. Bankdaten, geistiges Eigentum oder Mitarbeiterdaten. Nach ISO/IEC 27005 findet noch eine Unterscheidung nach primären Assets, die bspw. unerlässlich für die Erreichung von Geschäftszielen oder geheimhaltungsbedürftige Prozessbestandteile enthalten, sowie unterstützende Assets, die durch mögliche Schwachstellen und Bedrohungslagen für die Primary Assets im Zuge einer Risikoanalyse relevant werden. Zu letzteren gehören bspw. Netzwerkstruktur und spezifische Software. Vgl. Klipper, Risk Management, S. 68 ff. (Zitat nach: KLIPPER, Risk Management, S. 17. Vgl. auch ebd., S. 68 ff.). Nach Definition des BSI werden Assets als „Bestände von Objekten bezeichnet, die für einen bestimmten Zweck, besonders zur Erreichung von Geschäftszielen, benötigt werden.“ Es wird weiterhin darauf verwiesen, dass die im deutschen gängige Übersetzung mit ‚Wert‘ eine Unschärfe beinhaltet (BSI, Leitfaden, S. 83). Die britischen Nationalarchive definieren information asset als „a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively“ (https://cdn.nationalarchives.gov.uk/documents/information-management/identify-information-assets.pdf, S. 10). Als Beispiele eines einzelnen *assets* werden genannt: *a database of contacts*, *all files associated with a specific project*, *all the financial data for an organisation*.

Information type	Hoe long to keep	Sensitivity	Where stored	Key corporate asset	Can be destroyed now	Data size
Strategic planning	Long term	FOIA exemptions	EDRMS	Yes	No	Small
Public complaints	Medium term	DPA	Standalone database	No	No	Small
Building plans	Long term	No	Paper files	Yes	No	Small
Project X	Short term	No	Shared drive	No	No	Small
Weblog files	Short term	DPA	Server Z	No	Yes	Large

Abb. 3: Beispielhafte *asset list* einer fiktiven Organisation nach Handreichung der TNA[56]

Prinzipiell kann man Risiko-Assessments auf der Basis einzelner Assets betreiben – in großen Organisationen stehen dafür auch gegebenenfalls die personellen Ressourcen bereit. In der Praxis dürften solche Kompilationen im deutschsprachigen Archivwesen bislang wenig verbreitet sein. Da Asset-gestützte Risikoanalysen zeitaufwendig sind, kann ein praktikabler Weg sein, sich auf solche *high value assets* zu konzentrieren, die besondere Risikofaktoren darstellen und für die es sich lohnt, individuelle Kontrollmaßnahmen zu prüfen – ähnlich wie es das Vorgehen nach IT-Grundschutz vorsieht.[57] Eine Datenklassifizierung, z.B. nach dem 3-stufigen Standard-Datenschutzmodell (SDM) oder dem 5-stufigen Schutzstufenkonzept des LfD Niedersachsen kann die Grundlage bilden, jene besonders schutzbedürftigen Daten in einem Archiv zu ermitteln.[58] Die Klassifizierungen reichen im Falle des niedersächsischen Konzepts von Stufe A („Daten, die von den Betroffenen frei zugänglich gemacht wurden“, bspw. eine selbst veröffentlichte Webseite) bis zu Stufe E („Daten, deren unsachgemäße Handhabung Gesundheit, Leben oder Freiheit des Betroffenen beeinträchtigen könnte“, zum Beispiel die Daten eines Zeugenschutzprogramms). Eine Abschätzung der wichtigsten Assets anhand einer Datenklassifizierung kann in einem Archiv ein wichtiger (Teil-)Schritt einer Risikoanalyse sein, da die Überlegungen zu Schadenswirkungen integraler Bestandteil des Vorgangs sind und sich Risiken aus der bereits genannten Formel von Schaden und Eintrittswahrscheinlichkeit ergeben. Zur Einschätzung von Eintrittswahrscheinlichkeiten bieten sich Überlegungen zu den gängigsten Handlungsmustern von Akteuren der Cyberkriminalität und ihrer Methoden an, die im Folgenden kurz angerissen werden sollen.

---

[56] Entnommen aus: https://cdn.nationalarchives.gov.uk/documents/information-management/identify-information-assets.pdf.

[57] CALDER/WATKINS, Information Security Risk, Chapter 3.

[58] https://lfd.niedersachsen.de/startseite/technik_und_organisation/schutzstufen/schutzstufen-56140.html; https://www.datenschutzzentrum.de/sdm/.

III. 4. Akteure, Motivationen und Methoden

Im eingangs erwähnten Report *identity of a nation* von Anne LYONS wird betont, dass im australischen Diskurs über Cybersicherheit die Systemkomponenten, darunter Hardware-, Software-, und Kommunikationssysteme, längst eingehender auf Schwachstellen untersucht worden sind, die Erfassung der Absichten und Motive (*intent*) von Cyberkriminellen dagegen kaum systematisch erfasst worden sind.[59] Für den allgemeineren Bereich des IT-Risikomanagements ist die Frage der Gefährder und ihrer Motivationen von zentraler Bedeutung:

> „Es ist eine Sache, ob man einen Hackerangriff als Risiko erkennt und eine andere ob man weiß, welche Motive den Hacker leiten und welche Auswirkungen sein Angriff haben könnte. Beschäftigt man sich nur mit dem Risiko Hackerangriff als solches, dann driftet man vom eigentlichen Problem ab und beginnt damit, die IT-Ausstattung abzusichern, statt sich mit den Geschäftsprozessen auseinanderzusetzen.“[60]

Als vorsätzlich agierende Akteure im Bereich der Cyberkriminalität können etwa folgende Gruppen unterschieden werden:[61]

- Kriminelle: Die nach übereinstimmenden Studien größte Gruppe sind primär finanziell motivierte Akteure. Das Spektrum reicht von Einzelakteuren ohne technische Kenntnisse (*cybercrime as a service*) bis hin zu professionell organisierter Kriminalität
- Wirtschaftsspione: Ziel ist die Gewinnung von geldwerten Vorteilen gegenüber Mitbewerbern durch Konkurrenzausspähung
- Staatliche Akteure (z.B. Nachrichtendienste): Diese zielen gegenüber der Wirtschaftsspionage weniger auf finanzielle Vorteile, sondern auf Informationsbeschaffung und Einflussnahme
- Terroristen: Zur Diskussion um terroristische Täter im Archivbereich sei auch auf die Ausführungen bei LANGE (2016) verwiesen
- Aktivisten: Akteure, die auf gesellschaftliche Missstände aufmerksam machen und durch Cyberangriffe diesbezügliche Forderungen durchsetzen wollen
- Statusmotivierte Gruppen (Hacker, Cracker, Skriptkiddies): Angriffe dienen vornehmlich der Anwendung und Verbesserung von Kenntnissen

Diese Gruppierungen lassen hinsichtlich ihrer Motivationen Überschneidungen zu und sind nicht abschließend zu verstehen. Als weitere Großgruppe sind Innentäter zu zählen, die sich hinsichtlich ihrer Motivation kaum systematisch strukturieren lassen. Aufgrund

[59] LYON, Identity.
[60] KLIPPER, Risk Management, S. 33.
[61] BSI, Cyber-Bedrohungen, S. 2 f.

ihrer intimen Kenntnisse von Sicherheitsstrukturen und Zugangsmöglichkeiten zu sensiblen Daten können Innentäter hinsichtlich des anzurichtenden Schadenfaktors ein erhebliches Sicherheitsrisiko darstellen; KLIPPER fordert in seinem Handbuch sogar eine Konzentration auf die Innentäter.[62] Denkbar sind auch im archivischen Bereich Mitarbeiter, die aus Rache digitale Sabotage betreiben, aus wirtschaftlichem Interesse handeln oder Taten begehen, um einen Kollegen anzuschwärzen. Für den verhältnismäßig kleinen und geschlossenen Berufsbereich der Archivare sollte man die Gefahr aber sicherlich nicht überstrapazieren, zumal im Gegensatz zu Wirtschaftsunternehmen der Aspekt der eigenen Bereicherung nur eine marginale Rolle spielen dürfte. Bei gängigen Arbeitsschritten in der digitalen Archivierung existieren in Form des Vier-Augen-Prinzips, Protokollierungen, Versionierungen und der Einbindung mehrerer zuständiger Mitarbeiter zudem Schutzmechanismen zur Wahrung der Vertrauenswürdigkeit von Daten. Für den Archivbereich liegen bislang keine Veröffentlichungen (und dem Verfasser keine Stellungnahmen aus den geführten Interviews) vor, aus denen ersichtlich wird, dass Täter gezielt aus der einen oder anderen Motivation heraus gezielte Angriffe auf ein Archiv getätigt haben. Bekannt sind Fälle, in denen Archive von den Auswirkungen von finanziell motivierten Ransomware-Angriffen auf die jeweils davor geschalteten Verwaltungen betroffen waren. In diesen Fällen stand weniger die Erbeutung von Daten des Archivs im Vordergrund, als dass die Einrichtungen durch die angebundenen Informationssysteme und verwaltungstechnische Entscheidungen in der Ausführung ihrer Aufgaben betroffen waren. Nimmt man diese mehrfach eingetroffenen Fälle als Grundlage der Erstellung von Kennziffern, sollte man sich auch im Archivbereich weiterhin auf den großen Bereich der finanziell motivierten Kriminellen konzentrieren. Dass sich je nach Bestand und Aufgabenbereich des Archivs darüber hinaus spezifische Gewichtungen ergeben (Wirtschaftsarchive/Wirtschaftsspionage), versteht sich von selbst.

Einen noch konkreteren Überblick über gängige Bedrohungslagen gewinnt man, wenn man zu den eher abstrakten Überlegungen bezüglich der Akteure die häufigsten Methoden von IT-basierten Angriffen hinzunimmt. Die folgenden Muster wurden auf der Basis verschiedener BSI-Register und diverser Literaturartikel zusammengestellt:[63]

- Einschleusen von Schadsoftware über Wechseldatenträger
- Infiltration per E-Mail, Social Engineering und Phishing

[62] „Vergessen Sie die Terroristen… Hacker, Kriminelle oder gar Terroristen stehen als Bedrohungsquelle nun mal nicht vor dem Innentäter“ (KLIPPER, Risk Management, S. 46).
[63] BSI, ICS. Vgl. auch DINIS, Bedeutung, S. 55 f.; BRECHTKEN et al., S. 67 ff.

- Gezielte Infektion mit Schadsoftware über Internet und Intranet
- Ungepatchte Anwendungssoftware
- Malware
- Ransomware
- Ungezielte Verteilung von Schadsoftware mittels Spam oder Drive-by-Exploits zur breitflächigen Infiltration von Rechnern
- Menschliches Fehlverhalten
- Interne bzw. externe Sabotage
- Kompromittierung von Extranet und Cloud-Komponenten
- DDoS-Attacken
- CEO-Fraud
- Technisches Fehlverhalten und höhere Gewalt
- Einbruch über Fernwartungszugänge
- Kompromittierung von Smartphones im Arbeitsumfeld
- Bring your own device (BYOD)

Aktualisierte Zusammenstellungen von den häufigsten und konkreten Problemen und Risiken finden sich weiterhin auch in den Veröffentlichungen des SANS-Institut und dem Annex D der ISO 27005.[64] Während diese generischen Problemstellungen bei Überlegungen zu Ursachenszenarien im Archiv hilfreich sein können, kommt man mangels verfügbarer Veröffentlichungen rasch an die Grenzen der Risiken archivspezifischer Geschäftsprozesse bzw. Schwachstellen.

III. 5. Konsequenzen und Schadensbilder

Versucht man die Konsequenzen des Verlustes oder der Kompromittierung von Informationen abzuwägen, kann z.B. auf die Blaupause der häufigsten Schadensbilder nach BSI-Grundschutz zurückgreifen:[65]

- Verstoß gegen Gesetze/Vorschriften/Verträge
- Beeinträchtigung des informationellen Selbstbestimmungsrechts
- Beeinträchtigung der persönlichen Unversehrtheit
- Beeinträchtigung der Aufgabenerfüllung
- negative Innen-oder Außenwirkung
- finanzielle Auswirkungen

Darüber hinaus können über diese allzu abstrakten Konsequenzen („beeinträchtige Aufgabenerfüllung“) auch Schadensparameter aus dem Katastrophenschutz herangezogen werden, um die Beeinträchtigung der Datenvertraulichkeit in digitalen Archiven abzuwägen. Hier bieten sich z.B. die immateriellen Schadensbilder der

[64] https://www.sans.org/blog/cis-controls-v8/. Vgl. KLIPPER, Risk Management, S. 50 f.
[65] BSI-Standard 200-2, S. 173 ff. Vgl. auch KFN, Cyberangriffe, S. 36 ff.

Methode für die Risikoanalyse nach dem Bundesministerium für Bevölkerungsschutz und Katastrophenhilfe (BBK) an.[66]

Bereich	Abkürzung	Schadensparameter	Erläuterung/ Operationalisierung	Maßeinheit
IM-MATERIELL	I1	Auswirkungen auf die öffentliche Sicherheit und Ordnung	Ausmaß der Auswirkungen des Ereignisses auf die öffentliche Sicherheit und Ordnung (z. B. öffentliche Proteste, Gewalt gegen Personen/Objekte)	Ausmaß
	I2	Politische Auswirkungen	Ausmaß der Auswirkungen auf den politisch-administrativen Bereich (z. B. Forderung nach staatlichem Handeln, öffentliche Rücktrittsforderungen)	Ausmaß
	I3	Psychologische Auswirkungen	Ausmaß des Vertrauensverlustes in staatliche Institutionen (z. B. Regierung/ öffentliche Verwaltung)	Ausmaß
	I4	Schädigung von Kulturgut	Durch das Ereignis geschädigtes Kulturgut gemäß Haager Konvention	Anzahl und Grad der Schädigung

Abb. 4: Beispielhafte Schadensparameter im Katastrophenmanagement nach BBK-Methode[67]

Das Treffen generischer Aussagen über die Konsequenzen für „ein Archiv an sich“ ist, wie bereits angesprochen, wenig zielführend; es bedarf der Einbeziehung der archivspezifischen Bestände und organisatorischen Einbindung. Am ehesten kann man sich allgemein gültigen Aussagen noch anhand von Negativbefunden nähern.

So kommt dem finanziellen Aspekt bei der Evaluierung von IT-Bedrohungen in der Literatur große Bedeutung zu, da diese hauptsächlich von wirtschaftlich handelnden Unternehmen ausgeht. Anhand dieses Parameters wird hauptsächlich gefragt, welche identifizierten Risiken ein Unternehmen einzugehen bereit ist bzw. welche Anpassungsleistungen im Falle nicht tragbarer finanzieller Risiken erbracht werden müssen. Im Bereich der öffentlich finanzierter Kultureinrichtungen gelten aber sicherlich andere Gewichtungen. Es ist fraglich, ob es für den Bereich der staatlichen Archive überhaupt katastrophale - im Sinne existenzbedrohender - Schadensbilder gibt. Kein staatliches Archiv wird wohl durch einen Cyberangriff in seiner Existenz in Frage gestellt und seiner rechtlichen Grundlage entzogen werden. Wenn man die Einbeziehung von IT-Dienstleistern und die Arbeitszeitverluste bei Sicherheitsvorfällen als finanzielle Schäden versteht, können sich hier aber sehr rasch auf die ganze Organisation erstreckende langfristige Konsequenzen ergeben. Auch eine Unterbrechung von (ggf. drittmittelfinanzierten) Projekten und aufeinander aufbauenden Posten in der

[66] BBK, Methode, S. 31. Vgl. auch LANGE, Terror, S. 16 f.
[67] Entnommen aus: BBK, Methode, S. 31.

langfristigen Finanzplanung eines Archivs müssen hierbei bedacht werden.

Fraglich ist hinsichtlich des rechtlichen Aspekts, ob die Novellierung im Datenschutz 2018 als Movens der Verbesserung der IT-Sicherheit im deutschen Archivbereich wirkt. Weithin angenommen wird, dass Bußgelder vonseiten der Datenschutzbeauftragten gegen öffentliche Einrichtungen kaum genutzte Sanktionsinstrumente sind.[68] Denn diese können nach § 43 Absatz 3 BDSG[69] und anderer landesrechtlicher Regelungen und Spezialgesetze nur in beschränktem Umfang zu Adressaten von Bußgeldern werden.[70] Entscheidend ist dabei die Tätigkeit, bei der die zu verarbeitenden Daten von der Behörde verwendet werden: auf das „Bußgeldprivileg“ können sich Behörden und öffentliche Institutionen nur dann verlassen, wenn die Verarbeitung der Daten ihrem gesetzlichen Aufgabenspektrum unterliegt. Präzedenzfälle scheinen für Archive jedenfalls bisher nicht vorzuliegen.

Im Bereich materieller Konsequenzen (Kulturgutverlust) wäre in einem digitalen Archiv ein gänzlicher Verlust der Primärdaten sicherlich das größte anzunehmende Schadensbild; er ist aufgrund der üblichen Konzeption der mehrfach redundanten Speicherungen indes sehr unwahrscheinlich. In vielen Archiven dürften jedoch potenziell archivwürdige Unterlagen existieren, die noch nicht ein digitales Endarchiv überführt wurden (z.B. unstrukturierte Fileablagen)[71] und dabei in einem hohen Maße anfällig für einen unwiderruflichen Datenverlust sind.

Tatsächliche Auswirkungen von Cyberangriffen haben sich in deutschen Archiven bislang vor allem in Arbeitszeitverlusten, in der Aufarbeitung der Schadensbilder und der Verunmöglichung der Weiterarbeit in entsprechenden Informationssystemen, einer betroffenen Überlieferungsbildung und konkreten Datenverlusten geäußert. Potenziell sollte daneben immer dem immateriell-psychologischen Aspekt der Außenwirkung eines Archivs Beachtung geschenkt werden.

IV. Meinungsbilder und Aussagen

Für einen Sachstand im Bereich des Umgangs mit IT-Risiken im Archivbereich wurden

[68] Vgl. die Fallsammlung unter: https://www.dsgvo-portal.de/dsgvo-bussgeld-datenbank.php.

[69] „Gegen Behörden und sonstige öffentliche Stellen im Sinne des § 2 Absatz 1 werden keine Geldbußen verhängt“ (https://dejure.org/gesetze/BDSG/43.html).

[70] Vgl. im Folgenden: https://www.kanzlei.de/gegen-oeffentliche-stellen-koennen-in-wichtigen-ausnahmefaellen-datenschutz-bussgelder-verhaengt-werden

[71] „Unter einer unstrukturierten Fileablage oder Dateisammlung wird eine Menge genuin digitaler Daten nicht näher bestimmten Typs verstanden, die in einer ebenfalls nicht näher definierten Ordnung in einem Verzeichnissystem abgelegt sind und dem Archiv in ihrer Gesamtheit, beispielsweise auf einem tragbaren Wechsel-Datenträger, angeboten werden. Solche Ablagen entstehen abseits der geregelten Aktenführung auch in Behörden, vor allem aber sind sie typisch für nicht-amtliche Überlieferungen, beispielsweise für digitale Nachlässe“ (LENARTZ, Digital, S. 16)

standardisierte Fragebögen (s. Anhang) an Institutionen in Deutschland und verschiedenen Nachbarländern geschickt sowie Interviews geführt. Die befragten Ansprechpartner sind in unterschiedlichen Informationseinrichtungen und auf verschiedenen Ebenen tätig – vom Kommunalarchivar, der weitestgehend für alle Aspekte der digitalen Archivierung im eigenen Haus zuständig ist, bis zum hauptamtlich beauftragten IT-Sicherheitsbeauftragten eines staatlichen Archivs. Dadurch haben sich unterschiedliche Gewichtungen und Schwerpunktsetzungen ergeben, zumal eine erklärte Zielsetzung der Interviews eine ergebnisoffene Herangehensweise an das Thema „Archivisches IT-Risikomanagement“ war. Da die Interviewpartner auf unterschiedlichen organisatorischen Ebenen verortet sind und sich die Datenbasis als insgesamt zu wenig repräsentativ herausgestellt hat, sollen im Folgenden einige Meinungsbilder wiedergegeben werden, die dem Verfasser bezüglich der Aspekte IT-Sicherheit/Risikomanagement/Kommunikation als wichtig erscheinen. Die im Folgenden aufgeführten Aussagen wurden zur Verdeutlichung und Anonymisierung z.T. paraphrasiert.

Meinungsbild 1: „IT-Sicherheit ist Angelegenheit der zuständigen IT-Abteilung.“ Archivare haben nicht die Kompetenzen und vor allem nicht die Kapazitäten neben der alltäglichen Arbeit, sich um Fragen der IT-Sicherheit zu kümmern.

Meinungsbild 2: „Archive definieren Anforderungen an Langzeitarchive, deren Umsetzung den IT-Spezialisten obliegt.“ Das Archiv definiert einige Anforderungen an die Sicherheit, woran man sich an den entsprechenden Normen orientiert, und deren technische Umsetzung von der zugeordneten IT-Abteilung umgesetzt wird. Durch Service-Level-Agreements können Regularien zu Sicherung und Vorgehen im Störungsfall vereinbart werden.

Meinungsbild 3: „Wir betreiben Risikomanagement gemäß ISO 27005“. Die Risikoanalyse konzentriert sich primär auf die Identifizierung von Bedrohungen (*threats*) und zu erwartender Folgen (*business consequences*) für die Einrichtung. Für inakzeptable Risiken werden Notfallpläne (*priority action plans*) erstellt. Eine detaillierte Asset-orientierte Risikoanalyse wird nicht vorgenommen.

Meinungsbild 4: „Unsere Daten sind nicht relevant genug für Cyberattacken.“ Aufgrund des Alters oder des spezifischen Inhalts der archivierten Datensätze würden die Primärdaten, auch wenn sie durch Provenienzzusammenhänge und Metadaten

angereichert sind, keine Bedeutung für gängige Bedrohungsmuster entfalten.

Meinungsbild 5: „Digitale Archivierung erfordert besondere Anforderungen an die Sicherheit.“ Im Gegensatz zu einem Einbruch in einem analogen Archiv, wobei im schlimmsten Falle der Erhalt oder die Authentizität einer Handvoll Akten in Mitleidenschaft geriete, könnten bei einem Sicherheitsvorfall in einem digitalen Archiv massenhaft personenbezogene Daten entwendet werden.

Meinungsbild 6: „Die Umsetzung der entsprechenden IT-sicherheitstechnischen Anforderungen erfolgt auf Basis der verwendeten Inhalte, deren Schutzniveaus nach Datenschutzklassifizierung vorgenommen werden“. Diese beinhaltet auch die Umsetzung der Bausteine nach BSI-Grundschutz.

Meinungsbild 7: „Standards zur Evaluierung der IT-Sicherheit sollen vertrauenswürdige digitale Archivierung unterstützen, und nicht zu einer Nicht-Umsetzung führen“. Standards und Kriterienkataloge, wie sie bspw. bei TRAC und der *nestor*-Zertifizierung nach DIN 31644 zu finden sind, könnten aufgrund fehlender Ressourcen zur Umsetzung abschreckend wirken. Anstatt die Messlatte hier zu hoch anzusetzen, sollten Versuche zur Umsetzung von strategischen Konzepten unterstützt werden.

Meinungsbild 8: „Man kann ein Risiko auch als Chance auffassen!“ Nach einem Sicherheitsdurchbruch in einer kommunalen Verwaltung ist der Zugriff auf die Erschließungssoftware eines Archivs noch nicht möglich, es werden Datenverluste in der Erschließung der letzten Jahre vermutet. Der Vorfall gilt als Startschuss, um bislang unsystematisch genutzte Erschließungsrichtlinien zu vereinheitlichen und zukünftig anzuwenden.

Meinungsbild 9: „Backup der wichtigsten Assets im Verbund?“ Für kleinere Archive seien Back-up-Lösungen nach dem Grundgedanken eines LOCKSS-Prinzip (Lots of Copies Keep Stuff Safe) zu erwägen. Es wären niedrigschwellige Zwischenlösungen schon ein wesentlicher Fortschritt, wenn man die Arbeitszeitverluste oder gar die Verhinderung der Weiterarbeit nach Datenverlusten bedenkt.

Meinungsbild 10: „Eine Verbesserung der Ressourcen bedeutet noch keine Verbesserung der IT-Sicherheit.“ Der Fachkräftemangel an IT-Experten stellt eine wesentliche Herausforderung in der Umsetzung von Sicherheitsstrategien im Archivwesen dar.

Meinungsbild 11: „Revisionssicherheit wird durch den Einsatz eines revisionssicheren Speichers, redundante, auch physisch/lokal getrennte redundante Speicherung, zusätzliche Protokollierung, Erhaltung der Informationen im Rahmen von Migrationen (durch Erhalt der Ursprungsrepräsentation und Vorgängerversionen) und ausführliche Dokumentation im Zuge der Übernahme hergestellt."

Meinungsbild 12: „Der größte anzunehmende Unfall wäre der physikalische Ausfall der Speichersysteme", was aufgrund der mehrfach redundanten und physisch getrennten Datensicherung unwahrscheinlich ist.

Meinungsbild 13: „Im Workflow der Übernahme elektronischen Archivguts sind immer mehrere Personen (z.B. Ingest-Manager und Archivar) involviert, sodass eine Verletzung der Datenintegrität [durch Innentäter] nicht gesehen wird."

Meinungsbild 14: „Archivaren kommt eine Mittlerfunktion zwischen IT-Spezialisten und Mitarbeitern einer Verwaltung zu". Die Archivare sollten frühzeitig Kontakt mit den Sicherheitsbeauftragten aufnehmen und ihre Anforderungen und ihre Positionierung innerhalb der Verwaltung kommunizieren. Im eingetretenen Notfall wird das Archiv – neben anderen Brandherden - als wenig prioritär gesehen.

V. Ergebnisse und Fazit

Diese Arbeit kann aufgrund ihres begrenzten Zeitrahmens und Zuschnitts nur ein essayistischer Mosaikstein und bestenfalls ein Denkanstoß sein, sich mit Strategien und Methoden des IT-Risikomanagements auch im archivischen Bereich zu befassen.

Risikomanagement ist eine Ressourcenfrage. Kein Archivar wird sich neben der alltäglichen Arbeit mit ausufernden theoretisch Trockenübungen über potenzielle Bedrohungslagen beschäftigen wollen oder können, zumal Archivarinnen und Archivare qua ihrer Ausbildung in aller Regel Generalisten sind, die im seltensten Fall auf tiefergehende IT-Kenntnisse zurückgreifen dürften (und hier ist der Verfasser der Arbeit keine Ausnahme). Es sollte aber in dieser Arbeit hoffentlich deutlich geworden sein, dass Risikomanagement nicht so sehr auf die Klärung technischer Detailfragen abzielt. IT-Handbücher und Normen geben nur übergreifende und häufig erstaunlich generische und technikneutrale Richtlinien vor; anders wäre das Verfassen von allgemein gültigen Referenzrahmen auch gar nicht möglich. Hier gilt: „Keine Technologie dieser Erde wird

ihre Sicherheitsprobleme lösen“[72]. Die Leistungserbringer in der IT haben nicht unbedingt genaue Vorstellungen darüber, welche Daten im Archiv archiviert werden und welche Geschäftsprozesse vor sich gehen. Die Frage nach Ursache und Wirkung, nach der Einschätzung des spezifischen Gefährdungspotentials der in einem Archiv vorhandenen Bestände, was ein Angreifer damit bezwecken kann und welche Folgen für die Institution zu erwarten sind, wird vornehmlich durch den Archivar erfolgen können. Die Bestimmung von Assets mit hohem Schutzbedarf und den in einem digitalen Archiv erforderlichen Geschäftsprozessen kann man nach dem „Bauchgefühl“ machen, und dies wird in vielen Fällen auch gute Ergebnisse leisten. Die Verwendung von empfohlenen Methoden zu einem systematischeren Vorgehen der Risikoanalyse und eine grundlegende Kenntnis von etablierten Begriffen kann helfen, Anforderungen an die Umsetzenden in der IT sowie an die Bereitstellenden von Personal und Ressourcen zu vermitteln. Mit den leicht zugänglichen Hilfsmitteln zur Risikoanalyse und zum IT-Grundschutz haben Archivare heutzutage zahlreiche modulare Werkzeugkästen zur Verfügung, um über archivspezifische Herausforderungen bei der Kuration der ihnen anvertrauten Daten nachzudenken. Der Ewigkeitsanspruch des Archivs und die aus der digitalen Archivierung resultierenden Zugriffsmöglichkeiten auf große Mengen an personenbezogenen Daten können diese nämlich durchaus von anderen (Kultur-)Einrichtungen unterscheiden.

Jedes Archiv, das digital archiviert, muss sich mit Fragen der Sicherheit seiner Bestände und Geschäftsprozesse auseinandersetzen. Cyberangriffe beeinflussen aber auch solche Archive, die in der digitalen Archivierung bislang nicht oder nur ansatzweise tätig sind. Da für die archivarische Arbeit unerlässliche Geschäftsprozesse, z.B. Archivinformationssysteme auf einer funktionierenden Informationstechnik beruhen und eine Rückkehr zum rein analogen Arbeiten in vielen Bereichen nicht mehr möglich ist, ist die Frage nach Kontingenz-Plänen für alle Einrichtungen von Bedeutung. Auch kleine Behörden und Archive können zu einem attraktiven oder beiläufigen Angriffsziel werden, und gerade diese dürfte es von der strukturellen und personellen Ausstattung her auch vor wesentliche Herausforderung stellen. Archivare sollten sich vergewissern, wie die vorgeschaltete Verwaltung bzw. IT-Struktur bei den häufigsten Angriffsmustern- und Motiven – v.a. finanziell motivierten Ransomware-Angriffen – reagiert und welche Auswirkungen auf die Erfüllung der archivischen Fachaufgaben zu erwarten sind.

[72] KLIPPER, Risk Management, S. 13, der im selben Kapital das noch schärfere Diktum von Bruce SCHNEIER („If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology“) zitiert.

Wünschenswert wäre für die Zukunft eine Zusammenarbeit von Kuratoren, Archivaren und IT-Sicherheitsbeauftragten, um den Konnex Archiv/IT-Sicherheit auf breiter Basis zu erarbeiten und Anforderungen zu kommunizieren, wie es im schon angesprochenen Beispiel Australien geschehen ist. Hier hat das eindringliche Plädoyer für die Bedeutung ihrer digitalen Bestände und der dringenden Notwendigkeit einer Verbesserung ihrer Cybersicherheit eine ganz reichhaltige Ernte getragen, die sich neben der finanziellen Ausstattung auch im Stellenwert und der Strahlkraft der Archive in der modernen Gesellschaft überhaupt zeigen dürfte.

Zusammenfassung / Abstract

Die Transferarbeit „Archivisches IT-Risikomanagement“ gibt einen Überblick über jüngere Entwicklungen von IT-basierten Gefährdungen auf öffentliche Einrichtungen und Archive. Es wird die Frage erörtert, wie sich Methoden und Begriffe des Risikomanagements, spezieller der Risikoanalyse, nutzbar machen lassen, um Sicherheitsherausforderungen der digitalen Archivierung erfassen zu können. Ein Hauptmerkmal kann dabei auf der Erfassung archivischer Assets mit hohem Schutzbedarf und archivspezifischer Geschäftsprozesse liegen. Der Mangel an Veröffentlichungen und der Vertraulichkeit des Themas wegen sind Einblicke von außen und eine übergreifende quantitative Datenauswertung bislang nur schwer möglich. Eine knappe Einarbeitung und eine Verwendung von in der Risikoanalyse gebräuchlicher Parameter (Assets, Bedrohungen, Motive, Schwachstellen, Schäden) sowie von Überlegungen anhand gängiger Gefährdungslagen z.B. nach IT-Grundschutz bietet sich im Bereich der digitalen Archive aber grundlegend an, um auf einem gemeinsamen Nenner mit den Beteiligten des organisatorisch-strukturellem Überbau und den Umsetzenden der IT sprechen zu können. Ausgehend von Fragebögen und Interviews mit in der digitalen Archivierung tätigen Experten wurden exemplarische Meinungsbilder zu Herausforderungen und Bedrohungslagen eingeholt.

Literaturverzeichnis

Die in den Fußnoten aufgeführten Kurztitel sind unterstrichen. Alle Links wurden zuletzt am 30.03.2022 abgerufen.

[ASIT, Sicherheitshandbuch] Zentrum für sichere Informationstechnologie - Austria (A-SIT) / Bundeskanzleramt (BKA) (Hrsg.), Österreichisches Informationssicherheitshandbuch, Version 4.3.1 (2022)

BARATEIRO, José, Designing Digital Preservation Solutions: A Risk Management-Based Approach, in: The International Journal of Digital Curation, Vol. 5, Iss. 1 (2010), S. 5-17

[BBK, Methode] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (Hrsg.), Methode für die Risikoanalyse im Bevölkerungsschutz (2010)

[BKA, Cybercrime] Bundeskriminalamt (Hrsg.), Cybercrime. Bundeslagebild 2020

[BRECHTKEN et al, Identifikation] Brechtken, Helmut / Lichtenthäler, Chris / Hoffmann, Dominique, Identifikation von Cyber-Risiken, in: Cyber Security in der Risikoberichterstattung. Praxisleitfaden für optimiertes IT-Risikomanagement, Berlin 2021, S. 67-99

BRUN, Yann et. al., La Sûreté du Patrimoine archivistique, 2nd Edition (2018)

BRYDE, Bendik / GONZÁLEZ, Roberto, Secure Data for the Future. A Risk Assessment, in: International Journal of Digital Curation Vol. 13, Iss. 1 (2018), S. 327-343

[BSI, Cyber-Bedrohungen] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.), Cyber-Bedrohungen – ein Einstieg v1.0 (2012)

[BSI, Grundschutz] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.), IT-Grundschutz-Kompendium, Bonn 2021

[BSI, Industrial Control System Security] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.), Industrial Control System Security: Top 10 Bedrohungen

und Gegenmaßnahmen v1.3 (2019)

[BSI, Lage] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.), Die Lage der IT-Sicherheit in Deutschland 2021

[BSI, Leitfaden] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.), Leitfaden zur Basis-Absicherung nach IT-Grundschutz

[BSI, Register] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.), Register aktueller Cyber-Gefährdungen und -Angriffsformen v2.0

[BSI-Standard 100-2] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.), BSI-Standard 100-2. IT-Grundschutz-Vorgehensweise, Version 2.0 (2008)

[BSI-Standard 200-2] BSI-Standard 200-2. IT-Grundschutz-Methodik, v. 1.0

BÜLOW, Anna E., Risk Management as a Strategic Driver for a Large Archive, in: Collections: A Journal for Museum and Archives Professionals, Vol. 5, Iss. 1 (2009), S. 61-71

[CALDER/WATKINS, Information Security Risk] CALDER, Alan / WATKINS, Steve (Hrsg.), Information Security Risk Management for ISO27001/ISO27002, Ely 2010

[CoreTrustSeal] CoreTrustSeal Standards and Certification Board (Hrsg.), CoreTrustSeal Trustworthy Data Repositories Requirements: Extended Guidance 2020–2022, Extendend Guidance Version 2.0

DINIS, Manuel, Bedeutung eines IT-Risikomanagementsystems in der Praxis in Zeiten der digitalen Transformation, in: Carola Rinker (Hrsg.), Cyber Security in der Risikoberichterstattung. Praxisleitfaden für optimiertes IT-Risikomanagement, Berlin 2021, S. 11-66

DONALDSON, Devan Ray / BELL, Laura, Security, Archivists and Digital Collections, in: Journal of Archival Organization 15(1-2) (Mai 2019), S. 1-19

[DSK, Risiko] Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz), Kurzpapier Nr. 18: Risiko für die Rechte und Freiheiten natürlicher Personen (2018)

DURANTI, Luciana, The InterPARES Trust Project (2013-2019): An Overview, in: Karen Anderson/Irmgard Christa Becker/Luciana Duranti (Hrsg.), Born Digital in the Cloud: Challenges and Solutions. Contributions to the 21. Archival Science Colloquium / International Symposium of InterPARES Trust (Veröffentlichungen der Archivschule Marburg – Hochschule für Archivwissenschaft Nr. 65), S. 13-30

FRANK, Rebecca, Disaster Planning and Trustworthy Digital Repositories, University of Michigan 2012

FRANK, Rebecca D., Risk in trustworthy digital repository audit and certification, in: Archival Science 22 (2021), S. 43-73

FUZEAU, Pierre, Records management: France in search of a direction, in: Records Management Journal Vol. 13, Nr. 3 (2003), S. 130-135

GLEIßNER, Werner, Grundlagen des Risikomanagements. Mit fundierten Informationen zu besseren Entscheidungen, München 2017³

HARICH, Thomas W., IT-Risikomanagement: Richtlinien, Dokumentation, Massnahmen, Heidelberg u.a. 2018²

KEITEL, Christian / SCHOGER, Astrid (Hrsg.), Vertrauenswürdige digitale Langzeitarchivierung nach DIN 31644, Berlin/Wien/Zürich 2013

[KFN, Cyberangriffe] DREIßIGACKER, Arne / SKARCZINSKI, Bennet von / WOLLINGER, Gina Rosa, Cyberangriffe gegen Unternehmen in Deutschland. Ergebnisse einer repräsentativen Unternehmensbefragung 2018/2019 (Kriminologisches Forschungsinstitut Niedersachsen e.V. / Forschungsbericht Nr. 152) (2020)

KLIPPER, Sebastian, Information Security Risk Management. Risikomanagement mit ISO/IEC 27001, 27005 und 31010, Wiesbaden 2015²

KLIPPER, Sebastian, Konfliktmanagement für Sicherheitsprofis. Auswege aus der „Buhmann-Falle“ für Informations- und IT-Sicherheitsbeauftragte, Datenschützer, CISOs und Co., Wiesbaden 2020³

KORTE, Ulrike / KUSBER, Tomasz / SCHWALM, Steffen, Vertrauenswürdiges E-Government – Anforderungen und Lösungen zur beweiserhaltenden Langzeitspeicherung, in: Irmgard Christa Becker u.a. (Hrsg.), E-Government und digitale Archivierung. Beiträge zum 23. Archivwissenschaftlichen Kolloquium der Archivschule Marburg (Veröffentlichungen der Archivschule Marburg – Hochschule für Archivwissenschaft Nr. 67), Marburg 2021, S. 53-96

KRÓL, Patrick, Relevanz von Cyber Security Controls im Zuge der Risikoberichterstattung, in: Cyber Security in der Risikoberichterstattung. Praxisleitfaden für optimiertes IT-Risikomanagement, Berlin 2021, S. 119-178

KÜBLER, Thomas, „Wie kommt das Digitale ins Archiv?“ – Erfahrungen aus dem Stadtarchiv Dresden, in: Monika Storm u.a. (Hrsg.), Transformation ins Digitale. 85. Deutscher Archivtag in Karlsruhe (Tagungsdokumentationen zum Deutschen Archivtag 20), Neustadt a. d. Aisch 2017, S. 89-98

LANGE, Richard, Terror und archivische Notfallvorsorge. Transferarbeit im Rahmen des Archivreferendariats für den höheren Dienst an der Archivschule Marburg (49. Wissenschaftlicher Lehrgang) (2016)

LENARTZ, Stephan, Digital ist besser? Möglichkeiten der automatisierten Aufbereitung und Bewertung von Fileablagen mit Python am Beispiel einer digitalen Fotosammlung (Veröffentlichungen des Landesarchivs Baden-Württemberg / Werkhefte Digital 1), Stuttgart 2020.

LYONS, Anne, Identity of a nation. Protecting the digital evidence of who we are (2018).

[nestor, Erläuterungen] nestor - Kompetenznetzwerk Langzeitarchivierung und Langzeitverfügbarkeit Digitaler Ressourcen für Deutschland / nestor-Arbeitsgruppe Zertifizierung (Hrsg.), Erläuterungen zum nestor-Siegel für vertrauenswürdige digitale

Langzeitarchive, Version 2.1 (nestor-materialien 17) (2019)

[NIST, Guide] National Institute of Standards and Technology / U.S. Department of Commerce (Hrsg.), Guide for Conducting Risk Assessments (2012)

[RCE, Risk Management] Rijksdienst voor het Cultureel Erfgoed / Cultural Heritage Agency of the Netherlands (Hrsg.), Risk Management for Collections, Amersfoort 2017

TUNE, David, Functional and Efficiency Review of the National Archives of Australia (2020)

WEINREICH, Uwe, Lean Digitization. Digitale Transformation durch agiles Management, Berlin/Heidelberg 2016

XIE, Sherry Li, A must for agencies or a candidate for deletion: A grounded theory investigation of the relationships between records management and information security, in: Records Management Journal Bd. 29 Nr. 1 /2 (2019), S. 57-85

In den Fußnoten vollständig zitierte Links

https://www.20minutes.fr/high-tech/2979367-20210217-cyberattaques-elysee-promet-1-milliard-euros-contrer-menace-croissante

https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Vorfaelle/Ukraine-Krise/Massnahmenempfehlungen_BSI_Ukraine.html?nn=1025778#download=1=

https://cdn.nationalarchives.gov.uk/documents/information-management/identify-information-assets.pdf

https://www.datenschutzzentrum.de/sdm/

https://dejure.org/gesetze/BDSG/43.html

https://www.deutschlandfunk.de/datenschutz-cyberangriff-auf-das-berliner-kammergericht-100.html

https://www.dpconline.org/handbook/institutional-strategies/risk-and-change-management

https://www.dsgvo-portal.de/dsgvo-bussgeld-datenbank.php.

https://www.dw.com/en/ukraine-russia-face-off-in-cyberwar/av-61089184

https://en.wikipedia.org/wiki/Digital_preservation#Specific_tools_and_methodologies

https://e-estonia.com/estonia-to-open-the-worlds-first-data-embassy-in-luxembourg/

https://euobserver.com/digital/138406

https://www.faz.net/aktuell/wirtschaft/digitec/erster-cyber-katastrophenfall-in-deutschland-landkreis-liegt-lahm-17431739.html

https://www.faz.net/aktuell/karriere-hochschule/immer-mehr-hackerangriffe-auf-forschung-und-universitaeten-16802500.html

https://gazeta.a42.ru/lenta/news/132786-roskomnadzor-v-rossii-rezko-vozroslo-kolicestvo-kiberatak-na

https://www.itnews.com.au/news/national-archives-gets-67m-to-digitise-records-boost-cyber-security-566785

https://www.kanzlei.de/gegen-oeffentliche-stellen-koennen-in-wichtigen-ausnahmefaellen-datenschutz-bussgelder-verhaengt-werden

https://landesarchiv.hessen.de/sites/landesarchiv.hessen.de/files/digitalstrategie_hla.pdf

https://lfd.niedersachsen.de/startseite/technik_und_organisation/schutzstufen/schutzstufen-56140.html

https://www.mz.de/lokal/koethen/alles-wird-teurer-folgen-des-cyberangriffs-kosten-landkreis-anhalt-bitterfeld-bis-zu-zwei-millionen-3322297

https://www.onlinesicherheit.gv.at/Themen/Experteninformation/Normen-und-Standards/ISO-IEC-27000.html

https://www.regjeringen.no/en/dokumenter/national-cyber-security-strategy-for-norway/id2627177/

https://www.sans.org/blog/cis-controls-v8/

Anhang: Fragebogen, internationale Version

1) What are security challenges that you consider specific to archives, and in particular to your digital repository?

2) Security has always been a core aspect of trustworthy digital curation. Has the emphasis of security for your repository changed more recently in your organization, for example through test cases or organizational and legal changes?

3) How would you describe the current discussion about security of digital repositories in your organization and in the archival discourse of your country?

4) Who is tasked with the safekeeping of digital data in your archive? Do you feel that archivists in your institution are sufficiently prepared for the tasks of and threats to digital curation?

5) Which frameworks and standards build the foundation of managing data security in your archive?

6) Standards like ISO 16363:2012 and certificates for trustworthy curation like the nestor-seal recommend risk management to evaluate risks and to implement strategies to mitigate risks to digital repositories. Are methods of risk management already implemented for your repositories (or are there plans to implement them)? If so, could you describe your methodological framework and approach? If not, what would you consider a manageable approach and productive for your archive (e.g. asset-based, threat-based, vulnerability-based)?

7) Are there audits or self-assessments to evaluate cyber security?

8) What would you describe as key components in the workflow of digital curation in your archive to ensure the integrity of data?

9) Are there additional measures to ensure the security of particularly sensitive data?

10) How many people are involved in the process of digital curation? Are there considerations about the possibility of manipulation of data by insiders (e.g. log-protocols, versioning, 4-eyes-method)?

11) The threat of cyberattacks to even smaller administrative authorities has increased substantially in the last years. Do you consider your archive adequately positioned to tackle current threats to data security? What are changes you would like to see implemented?