API

OPEN ACCESS

Publiziert im Januar 2021
DOI: 10.15460/apimagazin.2021.2.1.64

Zeitschriftenartikel

Begutachtet

Begutachtet:

Prof. Christine Gläser
HAW Hamburg
Deutschland

Erhalten: *03. Januar 2021*

Akzeptiert: *18. Januar 2021*

Publiziert: *28. Januar 2021*

Empfohlene Zitierung:

GOLLAN, Lutz, 2021: Informationssicherheit – Grundlagen für Bibliotheken: Praxis-Überblick über den IT-Grundschutz-Standard. In: *API Magazin* **2**(1) [Online] Verfügbar unter: DOI 10.15460/apimagazin.2021.2.1.64

Informationssicherheit – Grundlagen für Bibliotheken

Praxisüberblick über den IT-Grundschutz-Standard

Dr. Lutz Gollan[1] [2]*

[1] Landesbetrieb Verkehr, Hamburg, Deutschland,
Fachbereichsleiter

* Korrespondenz: redaktion-api@haw-hamburg.de

Zusammenfassung

Für das Handlungsvermögen einer Bibliothek ist die Sicherheit der von ihr verarbeiteten Informationen zentral. Viele Einrichtungen wissen aber nicht, welche Daten verarbeitet werden oder wie es um deren Sicherheit bestellt ist. Mithilfe eines strukturierten Vorgehens auf Basis etablierter Standards kann Schritt für Schritt und nachvollziehbar dargelegt werden, ob die Vertraulichkeit, Integrität und Verfügbarkeit der Informationen und der diese verarbeitenden Systeme ausreichend gewährleistet sind. Der Beitrag stellt exemplarisch vor, wie eine Bibliothek ihre Informationssicherheit nach dem Standard IT-Grundschutz 200-2 des Bundesamtes für Sicherheit in der Informationstechnik dokumentieren kann.

Schlagwörter: Informationssicherheit, Computer, Datenverarbeitung, Informationen, Praxis, Bibliotheken

Abstract

The security of the information processed in a library is central to its ability to act. However, many institutions do not know which data is being processed or what the status of their security is. With the help of a structured procedure based on established standards, it can be demonstrated step by step and comprehensibly whether the confidentiality, integrity and availability of the information and the systems processing it are adequately guaranteed. The article presents an example of how a library can document its information security in accordance with the IT-Grundschutz 200-2 standard of the German Federal Office for Information Security.

Keywords: Information Security, Computer, Information Processing, Information, Praxis, Library

2 Die Ausführungen geben ausschließlich die private und persönliche Meinung des Autoren wieder.

 DOI: 10.15460/apimagazin.2021.2.1.64

1 Einleitung

In Hochschulen, Behörden, Bibliotheken und anderen Bildungsinstitutionen, aber auch in der Wirtschaft, werden regelmäßig Informationen verarbeitet. Sie sind das „Öl" dieser Einrichtungen und sowohl Kerninhalt als auch Steuerungswerkzeug zur Verarbeitung der Inhalte. Ohne die Gewährleistung der Sicherheit drohen Stillstand, Missbrauch, Verlust und Manipulation. Damit wären ein verlässliches Arbeiten, Lehren und Forschen nicht mehr möglich. Wie kann eine solche Verlässlichkeit garantiert werden? Dies soll die Gewährleistung der *Informationssicherheit* leisten.

„Informationssicherheit" ist dabei der Zustand, in dem die drei Sicherheitsziele *Vertraulichkeit*, *Integrität* und *Verfügbarkeit* (siehe unten) für Informationen jeglicher Art im für die verantwortliche Stelle erforderlichen Maße durch angemessene technische und organisatorische Maßnahmen gewährleistet werden. Um den Zustand und die Wirksamkeit dieser Maßnahmen festzustellen, wurden weltweit und auch in Deutschland Standards entwickelt, die zum einen ein strukturiertes Vorgehen zur Zustandserhebung vorschlagen und zum anderen bestimmte Maßnahmen mehr oder weniger konkret empfehlen. Dadurch kann auch gesetzlichen Dokumentationsanforderungen, z.B. nach Artikel 5 Absatz 2 Datenschutz-Grundverordnung,[1] der eine Nachweispflicht für die Einhaltung der datenschutzrechtlichen Anforderungen etabliert, entsprochen werden.

Die Etablierung und der Betrieb eines Informationssicherheitsmanagement-Systems müssen dabei durch die Leitung der Einrichtung u.a. über den Aufbau und die Unterstützung einer entsprechenden Informationssicherheitsorganisation unterstützt werden.

Die Entscheidung für einen bestimmten Standard hängt u.a. von der Komplexität des sog. „Informationsverbundes" (siehe unten), also der Einrichtung und der von ihr verarbeiteten Informationen und deren Kritikalität ab. Mittlerweile gibt es eine Vielzahl von Standards und abgestufter Vorgehensmethoden.

Dieser Beitrag stellt exemplarisch das Vorgehen in einer öffentlichen Bibliothek gemäß des in Deutschland weit verbreiteten IT-Grundschutz-Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI), konkret BSI-Standard 200-2, dar (BSI 2017a). Neben den zentralen Katalogsdaten werden in einer Bibliothek u.a. Bestellinformationen, aber auch die Daten der Kundinnen und Kunden und der Beschäftigten verarbeitet. Dazu kommen die (weiteren) finanziellen und organisatorischen Informationen, die ebenfalls nicht schutzlos sein dürfen.

1 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119 vom 04.05.2016, S. 1- 88 [ELI: https://data.europa.eu/eli/reg/2016/679/oj].

 DOI: 10.15460/apimagazin.2021.2.1.64

Andere in Deutschland gebräuchliche Standards zur Dokumentation der Informationssicherheit durch sog. Informationssicherheitskonzepte sind u.a. VdS 10000[2], ISIS12[3] und ISO 27000[4]. Diese Standards sind unterschiedlich detailliert und komplex; für den Einstieg sind neben dem BSI-Standard in der Ausprägung der Vorgehensweise „Basis-Absicherung" aufgrund ihrer geringeren Komplexität und hohen Praxisnähe die VdS- und die ISIS12-Werke zu empfehlen.[5]

2 Wie unterscheiden sich IT- und Informationssicherheit und der Datenschutz? Was ist ein Informationsverbund?

Die *Informationssicherheit* bezieht sich auf Informationen jeglicher Art und Form, unabhängig davon ob, sie in Dateien oder Aktenordnern abgelegt und verarbeitet werden. Die *IT-Sicherheit* stellt eine Untermenge der Informationssicherheit dar. Sie betrachtet nur Informationen, die mithilfe und in informationstechnischen Systemen verarbeitet werden. Sie erfasst also nicht die papiergebundene Aktenverarbeitung. Der *Datenschutz* hingegen stellt eine *inhaltliche* Auswahl der Informationen in den Vordergrund: nur solche, die einen Bezug zu einer natürlichen Person haben, also die Identifizierung eines Menschen ermöglichen (könnten). Die Informationssicherheit umfasst diese Unterbegriffe.

Der *Informationsverbund* ist der Begriff für eine örtlich und sachlich abgrenzte Organisation, z.B. eine Behörde oder ein Unternehmen, die von den Verantwortlichen als Betrachtungsobjekt bestimmt wird. Es können auch Untereinheiten, z.B. eine Stadtteilbibliothek, als Informationsverbund bestimmt werden. Er sollte so eng definiert sein, dass die Überschaubarkeit der betrachteten Elemente gewährleistet ist, aber weit genug, um zumindest die wichtigsten Geschäftsprozesse der Organisationseinheit mit zu erfassen. Grundsätzlich können jede Organisation und jede Untergliederung als Informationsverbund frei gewählt werden. So kann eine städtische Bibliothek in ihrer Gänze mit allen ihren Standorten als Informationsverbund bestimmt werden, aber ggf. auch nur eine einzelne Zweigstelle oder die Hauptstelle.

Die oben genannten Standards sind grundsätzlich für alle Informationsverbünde nutzbar. Im Folgenden wird nach einer Darstellung allgemeingültiger Eckpunkte der IT-Grundschutz 200-2 näher betrachtet.

2 Vormals VdS 3473; https://vds.de/kompetenze/cyber-security/zertifizierung/informationssicherheit-fuer-kmu-vds-10000 [Zugriff am 2020-12-28].
3 https://isis12.it-sicherheitscluster.de [Zugriff am 2020-12-28].
4 https://www.iso.org/standard/73906.html [Zugriff am 2020-12-28].
5 Ein tabellarischer Vergleich befindet sich in der Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen (Deutscher Landkreistag 2017, S. 9).

 DOI: 10.15460/apimagazin.2021.2.1.64

3 Welche Schritte sind den Standards gemein?

(Fast) allen Standards ist gemein, dass zunächst abgegrenzt werden muss, was untersucht und dokumentiert werden soll: Der Informationsverbund wird definiert. Das Ziel ist, dass den Verantwortlichen der betroffenen Einrichtung nachvollziehbar bekannt ist, welche Informationen im betrachteten Verbund verarbeitet werden und wie es um deren Sicherheit gemäß der Schutzziele bestellt ist. Nur so kann entschieden werden, ob die vorhandenen Maßnahmen ausreichen oder ob nachzusteuern ist.

Regelmäßig wird dabei im Anschluss an die Abgrenzung des Informationsverbundes eine Inventarisierung (sog. Strukturanalyse) durchgeführt. Darauf basierend wird erhoben, welches Schutzniveau für dieses „Inventar“ angemessen ist (Schutzbedarfsfeststellung). In der Folge müssen die nach dem jeweiligen Standard erforderlichen Maßnahmen bzw. Anforderungen dem Inventar und dem Schutzbedarf zugeordnet werden (Modellierung). Erst dann erfolgt die Prüfung, ob diese Maßnahmen erfüllt sind (Check). Das Ergebnis ist ein Bericht, der den Zustand der Informationssicherheit und ggf. offene Punkte darstellt. Es obliegt der Leitung der Einrichtung, diesen Bericht zur Kenntnis zu nehmen und, falls erforderlich, Abhilfe bei Lücken zu veranlassen. Im Folgenden werden die genannten Schritte erläutert.

Dieses Vorgehen ist regelmäßig zu wiederholen – es handelt sich um einen wiederkehrenden Prozess mit festen Zuständigkeiten (z.B. über eine*n Informationssicherheitsbeauftragte*n), nicht um ein einmaliges Projekt. Bei erheblichen Änderungen in der Struktur der Einrichtung, der verarbeiteten Informationen oder geänderter Schutzniveaus sind unterjährige Wiederholungen erforderlich.

Dabei stehen am Markt diverse IT-basierte Informationssicherheitsmanagement-Verfahren zur Dokumentation auf Basis der verschiedenen Standards bereit.[6] Ohne diese ist eine nachvollziehbare und effiziente Darstellung der Informationssicherheit einer Einrichtung praktisch nicht möglich. Einige der Anwendungen unterstützen dabei – mehr oder weniger stark integriert – auch die Dokumentation des Datenschutzes, z.B. über die teil-automatisierte Erzeugung des Verzeichnisses von Verarbeitungstätigkeiten gemäß Artikel 30 Datenschutz-Grundverordnung.

3.1 Schutzziele

Das Vorgehen orientiert sich dabei grundsätzlich an den Schutzzielen der Informationssicherheit. Dabei ist es gleichgültig, ob es sich bei den betrachteten

6 Vgl. die Übersicht unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Profile/Profile/itgrundschutzProfile_Profile_node.html [Zugriff am 2020-12-28].

 DOI: 10.15460/apimagazin.2021.2.1.64

Informationen um personenbezogene Daten, wie z.B. Name oder Anschrift von Kund*innen, oder anonyme Daten (z.B. statistische Auswertungen) handelt.[7] Auch nicht-personenbeziehbare Daten, wie etwa der Haushaltsentwurf einer Kommune oder Patent-Entwürfe, können ein wichtiges Gut der Einrichtung darstellen, das zu schützen ist. In einer Bibliothek stellen die nicht-personenbezogenen Informationen über den Bestand, aber auch die personenbezogenen Beschäftigten- und Kund*innendaten zentrale Werte da, die es zu schützen gilt.

Eines der drei zentralen Schutzziele ist die *Vertraulichkeit* der Informationen. Vertraulichkeit liegt vor, wenn nur befugte Personen Zugriff auf die Informationen haben. Die *Integrität* der Informationen ist ein weiteres Schutzziel. Dabei geht es um das Verhindern unbemerkter Veränderungen. Veränderungen sind regelmäßig statthaft und gewünscht – jedoch nur im Rahmen des von den verantwortlichen Personen Gewünschten bzw. Erlaubten. Manipulationen durch Unbefugte gefährden die Integrität und damit die Verlässlichkeit der Daten. Schließlich ist die *Verfügbarkeit* ein Schutzziel. Nur wenn die Informationen und die sie verarbeitenden Systeme wie vorgesehen tatsächlich genutzt werden können und nicht etwa durch Systemausfälle „offline“ sind, sind sie auch sicher im Sinne der Informationssicherheit.

3.2 Beispielhaftes Vorgehen nach BSI-Standard 200-2

Das Bundesamt für Sicherheit in der Informationstechnik ist eine Bundesbehörde und sieht sich als der zentrale IT-Sicherheitsdienstleister des Bundes. Seine Grundlagen sind nach eigener Aussage Fachkompetenz und Neutralität (BSI o. J.). Es hat den IT-Grundschutz als Standard entwickelt, der laufend gepflegt wird. Der im Jahr 2017 vollständig überarbeitete IT-Grundschutz-Standard 200-2 (Methodik) hat zum Ziel, flexibel über unterschiedliche Vorgehensweisen eine nachvollziehbare Dokumentation der Informationssicherheit in einer Einrichtung bzw. in einem Informationsverbund zu erhalten. Die alternativen Vorgehensweisen *„Basis-Absicherung“*, *„Kern-Absicherung“* und *„Standard-Absicherung“* ermöglichen den verantwortlichen Personen sich für eine für die Einrichtung angemessene Breite und Tiefe des Informationssicherheitskonzepts zu entscheiden.

Die *Basis-Absicherung* liefert die Grundlage, um in der Breite eine unspezifische Mindest-Absicherung des Informationsverbundes zu erreichen und dürfte für viele Institutionen den ressourcenmäßig sparsamsten Einstieg bieten (BSI 2017b). Die *Kern-Absicherung* hingegen wirft den Blick nicht in die Breite, sondern betrachtet die kritischen Geschäftsprozesse der Einrichtung, wenn man so will: die „Kronjuwelen“, und diese wiederum in aller Tiefe. Die *Standard-Absicherung* verlangt eine vollständige Betrachtung sowohl in der Breite als auch in der Tiefe und stellt den Gold-Standard des BSI dar.

7 Zum technischen Datenschutz siehe (Gollan 2019, S. 657).

 DOI: 10.15460/apimagazin.2021.2.1.64

Allen Vorgehensweisen ist die Methodik einer schrittweisen Abfolge der Dokumentation über *Strukturanalyse*, *Schutzbedarfsfeststellung*, *Modellierung* und *IT-Grundschutz-Check* gemein. Im Anschluss müssen ggf. *Umsetzungen* von Maßnahmen zur Erhöhung der Informationssicherheit erfolgen. Dabei bieten sog. IT-Grundschutz-Profile insbesondere für den Schritt „Modellierung" branchenrelevante Sub-Sets tauglicher Maßnahmen der adressierten Einrichtungen, z.B. im Profil „Basis-Absicherung Kommunalverwaltung".[8]

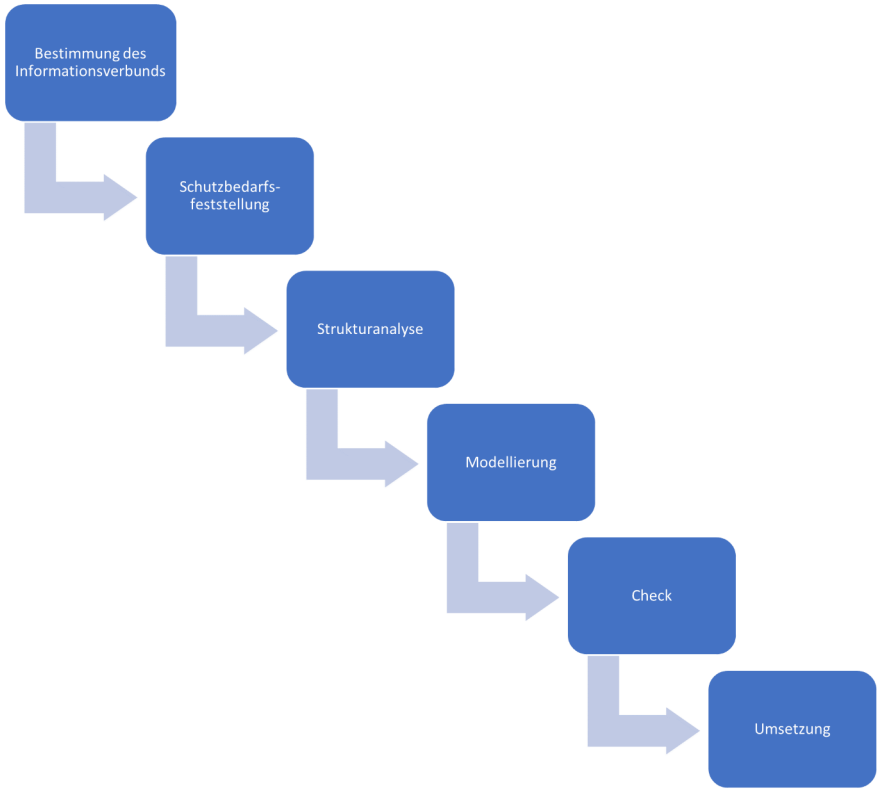

Abb. 1 Vorgehen nach BSI IT-Grundschutz 200-2 (eigene Darstellung)

3.2.1 Ersterfassung bzw. Strukturanalyse

Nachdem Klarheit über den zu dokumentieren Informationsverbund (z.B. nur eine Zweigstelle oder die gesamte Bibliothek) und die Vorgehensweise (z.B. die Basis-Absicherung) besteht und von der Leitung bestätigt wurde, ist eine Inventarisierung aus Sicht der Informationssicherheit vorzunehmen. Während nur die Standard- und die Kernabsicherung nach BSI-Standard 200-2 eine formale Strukturanalyse verlangen, soll für die Basis-Absicherung die Ersterfassung der Prozesse, Anwendung und IT-Systeme genügen (BSI 2017a, S. 26; 69; 77). Aus Sicht des Autoren ist diese Unterscheidung mehr redaktioneller Art. Auch für die Basis-Absicherung müssen die sog. Assets unter den gleichen Aspekten der Strukturanalyse erhoben werden. „Assets" sind die eingesetzten Informationen, Infrastrukturen und IT-Systeme etc. der Einrichtung, die deren Werte bilden.

8 Siehe die laufend erweiterte Übersicht unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzProfile/Profile/itgrundschutzProfile_Profile_node.html [Zugriff am 2020-12-28].

 DOI: 10.15460/apimagazin.2021.2.1.64

Dazu zählen neben den Standorten, Gebäuden, Stockwerken und Räumen die (Geschäfts-) Prozesse sowie Anwendungen und die von ihnen verarbeiteten Daten, die genutzten IT-Systeme inkl. Server und Endgeräte, und die Kommunikationsnetze. Dabei sollten stets verallgemeinernde Gruppen gebildet werden. Zum Beispiel wird nicht jeder einzelne Arbeitsplatzrechner dokumentiert, sondern nur eine Gruppe von gleich konfigurierten Geräten und deren standardmäßige Verortung (z.B. Sachbearbeitungsbüro). Über baumartige Strukturen wird so dargestellt, welche einzelnen Komponenten für einen (Geschäfts-) Prozess genutzt werden. Zum Beispiel: Es werden für den Vor-Ort-Prozess der Medienausleihe einer Bibliothek Kund*innen- und Medien-Daten über Kiosk-PCs mit Internet-Browsern in öffentlich zugänglichen Räumen im Erdgeschoss der Liegenschaft Marktplatz 10 mit Anbindung an den OPAC auf zentral gehosteten Anwendungs-Servern mit angeschlossenen Datenbank-Servern über das interne Netzwerk mit lokalem Drucker verwendet.

Für die Strukturanalyse oder Ersterfassung müssen diverse Stellen der Einrichtung mit einbezogen werden, um das gesamte Bild abzufragen und darzustellen, z.B. die IT-Abteilung.

3.2.2 Schutzbedarfsfeststellung

Für die Basis-Absicherung ist die Feststellung des Schutzbedarfs nicht erforderlich, da die geforderten Maßnahmen universell sind. Für die Kern- und die Standard-Absicherung wäre anhand der Schutzziele zu prüfen, ob ein normaler, hoher oder sehr hoher Schutzbedarf für die Assets besteht – danach richten sich die später auszuwählenden Maßnahmen. Die einzelnen Assets leiten ihren Schutzbedarf dabei vom jeweils sensibelsten in der Kette ab. Wird z.B. eine Information mit sehr hohem Schutzbedarf auf einem PC verarbeitet, so hat auch dieser einen sehr hohen Schutzbedarf. In Büchereien und Bibliotheken dürfte regelmäßig ein normaler Schutzbedarf vorliegen. Ein hoher Schutzbedarf wäre etwa anzunehmen, wenn der Verlust von Daten die Existenz der Einrichtung gefährden würde – oder wenn besonders sensible Daten wie über die Gesundheit von Kund*innen verarbeitet würden.

3.2.3 Modellierung

Nach dem die Struktur- und ggf. auch die Schutzbedarfsanalyse durchgeführt und dokumentiert wurde, sind den einzelnen Assets die sog. Bausteine des IT-Grundschutzstandards und des dazugehörenden „IT-Grundschutz-Kompendiums“ 1 mit den erforderlichen Maßnahmen zuzuordnen. Im Kompendium ist für fast alle denkbaren Assets dargelegt, wie z.B. ein Datenbank-Server oder ein Server-Raum abgesichert sein sollte. Gute Dienste erweisen dabei die oben erwähnten einrichtungsspezifischen IT-Grundschutz-Profile (soweit vorhanden). Da es aktuell noch kein Profil für Bibliotheken gibt, ist auszuwählen, welcher Baustein, z.B.

 DOI: 10.15460/apimagazin.2021.2.1.64

SYS.2.2.3: Clients unter Windows 10, für welches Assets der Einrichtung zu betrachten ist. Idealerweise nimmt einem die verwendete IT-Anwendung zur Erstellung des Informationssicherheitskonzeptes (siehe oben) diese Modellierung ab. Über die Auswahl der Vorgehensweise und andere Filter sollte die Software dann nur die relevanten Bausteine anzeigen und den Assets automatisch zuordnen. Bei der Basis-Absicherung bzw. bei Auswahl eines bestimmten IT-Grundschutz-Profils sind so nur die entsprechend gekennzeichneten bzw. ausgewählten wenigen Bausteine und Maßnahmen relevant und dem Informationsverbund automatisch zugeordnet.

3.2.4 IT-Grundschutz-Check

Im folgenden Schritt wird überprüft – im Beispiel durch die Bibliothek –, ob die Maßnahmen, die aufgrund der Modellierung zu betrachten sind, tatsächlich im Betrieb umgesetzt, fehlend oder ggf. geplant sind. Dies ist regelmäßig die aufwändigste Arbeit, die auch nicht im stillen Kämmerlein erledigt werden kann. Vielmehr sind über Interviews, je nach Umfang, Erreichbarkeit und Verständnis für die Fragen textbasiert oder persönlich / telefonisch, die für die fachliche und die technische Betreuung zuständigen Organisationseinheiten der Einrichtung aktiv zu befragen. Ansprechpartner*innen sind die IT-Abteilung, aber auch Fach-Abteilungsleitungen oder die zentralen Dienste (Facility Management etc.). Es wird dabei dokumentiert, ob die Maßnahmen gemäß den Bausteinen des Standards tatsächlich umgesetzt sind, z.B. ein Datensicherungskonzept für die Serverdaten besteht, wo dieses zu finden ist und ob es aktuell gehalten bzw. über Übungen auf Angemessenheit überprüft wird. Es empfiehlt sich vor Beginn des Checks sich der vollständigen Unterstützung der Leitung der Einrichtung zu vergewissern. Andernfalls kann es zur schleppenden Beantwortung der Fragen zum IST- und zum Planungsstand kommen.

Die Ergebnisse des IT-Grundschutz-Checks werden vermerkt – dadurch wird offenbar, wo es ggf. Lücken gibt und (weitere) Maßnahmen noch umzusetzen sind.

3.2.5 Umsetzung offener Maßnahmen

Im Normalfall wird der Check eine Vielzahl von Maßnahmen aufzeigen, die noch nicht oder nicht vollständig in der Einrichtung umgesetzt sind. Diese sind zu bewerten unter den Aspekten *Effektivität*, *Eignung*, *Praktikabilität*, *Akzeptanz* und *Wirtschaftlichkeit* (BSI 2017b, S. 63). Die Maßnahmen mit der höchsten Effektivität, die geeignet, praktikabel und von den betroffenen Personen akzeptiert werden, sollten als erstes in die Umsetzung gehen – vorausgesetzt, sie sind wirtschaftlich. Mangelt es an der Wirtschaftlichkeit, so sind Ersatzmaßnahmen zu prüfen, z.B. über Outsourcing. Eine mögliche Maßnahme ist die Einführung einer Verschlüsselung der Datenbanken, zumindest der mit den personenbezogenen Daten der Kund*innen. Aber auch eine Reduzierung der verarbeiteten Informationen könnte den Schutzbedarf und damit Aufwände für die erforderlichen Maßnahmen senken.

 DOI: 10.15460/apimagazin.2021.2.1.64

Sollten noch kleinere, leicht umzusetzende Maßnahmen offen sein, so sind diese ggf. unter zeitlichen Gesichtspunkten vorzuziehen, bevor z.B. langwierige Beschaffungsvorgänge für komplexere Punkte gestartet werden müssen.
Stets sollte der Umsetzungsplan von der Leitung der Einrichtung bestätigt werden. Sie trägt (auch) für die Informationssicherheit die Verantwortung und behält sich ggf. andere Prioritäten vor. Sie kann auch (sicher dokumentiert) entscheiden, dass eine Gefahr ohne Gegenmaßnahme akzeptiert wird oder der mögliche – finanzielle – Schaden durch eine Gefahr über den Abschluss einer Versicherung abgeschwächt wird.

4 Ergebnis

Die Erhebung und Dokumentation des Zustands der Informationssicherheit in Bibliotheken darf kein Selbstzweck sein, sondern beides dient dazu zu erkennen, welche Lücken es gibt, welche Gefahren drohen und welche Maßnahmen zu deren Abwendung sinnvoll und umsetzbar sein. Diese Sicherheit lässt sich nicht finanziell bemessen, wenn sie fehlt drohen jedoch erhebliche Schäden, u.a. durch Wiederherstellungskosten. Dazu treten ggf. Imageverlust, Haftung, Mehraufwände für Beschaffungen oder Korrekturen.

Die Verwendung von Standards für die Dokumentation erleichtert diese Arbeit. Anhand vorgegebener und idealerweise durch schlaue Software unterstützter Vorgehensweisen wird Schritt für Schritt und nachvollziehbar dargestellt, welches Inventar, welche Assets, die betrachtete Einrichtung nutzt und wie diese zu schützen sind. Dabei werden Mängel offenbar. Der Leitung der Einrichtung obliegt es dann zu entscheiden, ob und wie diese Lücken zu schließen sind.

Dieses Vorgehen sollte dabei um einen weiteren Rahmen ergänzt werden. Die Informationssicherheit muss dauerhaft organisatorisch etabliert werden, z.B. über die Bestellung eines*einer Informationssicherheitsbeauftragten oder eines Teams. Auch sollte eine Informationssicherheitsleitline durch die Leitung der Einrichtung verabschiedet werden, um den Stellenwert zu verdeutlichen und in der Organisation zu verankern (vgl. die Handreichung Deutscher Landkreistag 2017).

Der vorliegende Beitrag betrachtet daher einen zentralen, aber gleichzeitig nur einen Teilaspekt auf dem Weg zu einer verlässlichen Informationsverarbeitung in öffentlichen und privaten Einrichtungen.

 DOI: 10.15460/apimagazin.2021.2.1.64

Literatur

BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (BSI), 2017a: *BSI-Standard 200-2 – IT-Grundschutz-Methodik*. [Online] Stand: 2017-11-15 [Zugriff am: 2020-12-28] Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_2.pdf?__blob=publicationFile&v=7

BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (BSI), 2017b: *Leitfaden zur Basis-Absicherung nach IT-Grundschutz*. [Online] Stand: 2017-10-20 [Zugriff am: 2020-12-28] Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Leitfaden_zur_Basis-Absicherung.pdf?__blob=publicationFile&v=3

BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (BSI), 2020: *IT-Grundschutz-Kompendium*. [Online] Stand: 2020-03-02 [Zugriff am: 2020-12-28] Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2020.pdf?__blob=publicationFile&v=6

BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (BSI), o. J.: *Unser Leitbild*. [Online, Zugriff am: 2020-12-28] Verfügbar unter: https://www.bsi.bund.de/DE/DasBSI/Leitbild/leitbild_node.html

DEUTSCHER LANDKREISTAG, 2017: *Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen*. [Online] Stand: 2017-03-21 [Zugriff am: 2020-12-28] Verfügbar unter: https://www.landkreistag.de/images/stories/publikationen/bd-%20129.pdf

GOLLAN, Lutz, 2019: Datensicherheit. In: Martin Zilkens, Lutz Gollan, Hrsg.: Datenschutz in der Kommunalverwaltung. Berlin: Erich Schmidt Verlag. S. 657-697. ISBN 978-3-503-18758-4