Einführung in die Informationssicherheit für Schulen

Handreichung für Schulträger und Schulen

Berlin, 31.01.2023

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Informationen zum Dokument

Urheberschaft

Herausgeber: PD – Berater der öffentlichen Hand GmbH

Friedrichstraße 149

10117 Berlin

Webseite: https://www.pd-g.de

Haftungsausschluss

Zielgruppe

Die vorliegende Handreichung und die dazugehörigen Quick-Check-Bögen richten sich an die für die Informationssicherheit an Schulen und bei Schulträgern Verantwortlichen. Wer verantwortlich für die Informationssicherheit in den Schulen ist, ist teilweise in den gesetzlichen Vorgaben der einzelnen Bundesländer geregelt und sollte vor der Umsetzung der Handreichung überprüft sowie festgelegt werden.

Daneben sind die Handreichung und die Quick-Check-Bögen für diejenigen Mitarbeitenden in den Schulen oder auf Schulträgerseite vorgesehen, die operativ für die Umsetzung von Aufgaben im Rahmen der Informationssicherheit zuständig sind. Für diese Zielgruppe, die IT-Umsetzungsverantwortlichen bei Schulträgern und Schulen, steht im Jahr 2023 eine weitere Handreichung zur vertiefenden Lektüre bereit – Titel: „Informationssicherheit Schule im IT-Betrieb: Erste Schritte“. In dieser Handreichung finden Umsetzungsverantwortliche weiterführende handlungspraktische Informationen und Hinweise für erste wirksame Absicherungsmaßnahmen entlang der Lebenszyklusphasen des IT-Betriebs.

Zielsetzung

Die vorliegende Handreichung bietet Ihnen in Verbindung mit den dazugehörigen Quick-Check-Bögen eine kompakte Einführung in das Thema Informationssicherheit für Schulen und Schulträger, orientiert am aktuellen *IT-Grundschutz-Kompendium des BSI*[1] in Verbindung mit dem *IT-Grundschutzprofil Basis-Absicherung Kommunalverwaltung* (Stand 01.02.2023)[2].[3] Darüber hinaus wird Ihnen das für die öffentliche Verwaltung in Deutschland maßgebliche Informationssicherheitsrahmenwerk IT-Grundschutz-Kompendium des Bundesamts für Sicherheit in der Informationstechnik (BSI) vorgestellt und die für die Basis-Absicherung nach BSI relevanten Schichten, Bausteine und Ziele erläutert. Anhand eines einfachen Vorgehensmodells werden erste notwendige Schritte für einen BSI-konformen, systematischen Aufbau von Informationssicherheitsmanagement für Ihre Schulen skizziert.

Mit Hilfe von zehn begleitenden Quick-Check-Bögen kann in kurzer Zeit der Ist-Stand und Umsetzungsgrad bezüglich des Informationssicherheitsmanagements für Schulen und/oder Schulträger ermittelt werden, um daraus notwendige Maßnahmen ableiten. Die Handreichung und Quick-Check-Bögen streben dabei ein Schutzniveau an, das der Basis-Absicherung der IT-Grundschutzvorgehensweise entspricht.

[1] Bundesamt für Sicherheit in der Informationstechnik [BSI] (2023): IT-Grundschutz-Kompendium, Reguvis Fachmedien GmbH, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4#download=1, abgerufen am 07. Februar 2023.

[2] Arbeitsgruppe Kommunale Basis-Absicherung [AG KOBA] (2022): IT-Grundschutz-Profil Basis-Absicherung Kommunalverwaltung, https://www.landkreistag.de/images/stories/themen/egovernment/220331_IT-Grundschutz-Profil.pdf, abgerufen am 23. November 2022.

[3] Derzeit wird von einer bundesweiten Arbeitsgruppe der kommunalen Spitzenverbände zudem ein IT-Grundschutzprofil „Basisabsicherung Schule“ erarbeitet. Die Veröffentlichung ist für die zweite Jahreshälfte 2023 geplant.

Aufbau der Handreichung

Die vorliegende Handreichung ist modular aufgebaut und enthält an geeigneten Stellen Verlinkungen zu den Kapiteln oder zu den Informationen im Anhang. Die Handreichung ist in drei zentrale Kapitel gegliedert, die aufeinander aufbauen, aber auch einzeln gelesen werden können. Das Kapitel 2, Schulträgertypen und Betriebsstrukturen, betrachtet die kommunalen Schulträgerstrukturen aus dem Blickwinkel des Betriebs schulischer IT-Netzwerke und der darin enthaltenen Komponenten.

Darüber hinaus werden im Kapitel 2 die zentralen Rollen im Bereich der Schul-IT und die damit verbundenen Aufgaben beschrieben. Anhand eines vereinfachten Netzwerkplans wird ein grundlegender Überblick über vorhandene schulische Netzwerk-Infrastrukturen aufgezeigt.

Im darauffolgenden Kapitel 3, Informationssicherheit für Schulträger und Schulen, werden die Bausteine der Informationssicherheit des *IT-Grundschutz-Kompendiums des BSI*[4] in Bezug auf das *IT-Grundschutzprofil Basis-Absicherung Kommunalverwaltung*[5] dargestellt. Die in dieser Handreichung enthaltene Überblicksdarstellung und der Vorgehensvorschlag beziehen sich ausschließlich auf das Ziel einer Basis-Absicherung gemäß dem BSI-Grundschutz. Mit Hilfe der in diesem Dokument enthaltenen Quick-Check-Bögen können Schulträger und Schulen die Umsetzung dieser ersten Stufe der Informationssicherheits-Aufgaben in Angriff nehmen.

Das Kapitel 4, Erste Handlungsempfehlungen bei Störungen, gibt zudem einen ersten Überblick über die möglichen zentralen Schritte des Notfallmanagements im Falle einer Störung der Informationssicherheit.

[4] Bundesamt für Sicherheit in der Informationstechnik [BSI] (2023): IT-Grundschutz-Kompendium, Reguvis Fachmedien GmbH, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4#download=1, abgerufen am 07. Februar 2023.

[5] Arbeitsgruppe Kommunale Basis-Absicherung [AG KOBA] (2022): IT-Grundschutz-Profil Basis-Absicherung Kommunalverwaltung, https://www.landkreistag.de/images/stories/themen/egovernment/220331_IT-Grundschutz-Profil.pdf, abgerufen am 23. November 2022.

1 Einleitung

Als am 6. Juli 2021 im Landkreis Anhalt-Bitterfeld (Land Sachsen-Anhalt) eine Erpressernachricht einging und zentrale Server sowie Anwendungen aufgrund eines unbemerkt installierten Schadprogramms (Verschlüsselungstrojaner) nicht mehr genutzt werden konnten, waren das Ausmaß des Schadens und die Tiefe, mit der die Erpresser in die IT-Systeme der Kommunalverwaltung vorgedrungen waren, noch nicht absehbar.

Bereits am 9. Juli musste der Landkreis den Katastrophenfall ausrufen, da die Kreisverwaltung zentrale Systeme und Anwendungen nicht mehr unter ihrer Kontrolle hatte und deshalb ihre Kernaufgaben nicht mehr erfüllen konnte.

Was war passiert? – Der Landkreis war Opfer eines professionellen, mehrstufigen Cyberangriffs geworden, die bereits einige Monate vorher begonnen hatte. Durch eine Reihe sogenannter Phishing-Mails, also gefälschter E-Mails, verschafften sich die Angreifenden Zugriff auf Passwörter und E-Mail-Accounts von Mitarbeitenden der Kreisverwaltung. Auf diese Weise konnten sie sich monatelang unbemerkt in den IT-Systemen bewegen.

Die Kreisverwaltung brauchte mehrere Monate, um wieder arbeitsfähig zu sein. Der finanzielle Schaden wurde laut dem Mitteldeutschen Rundfunk auf rund 2 Millionen Euro geschätzt.[6] Dazu kommt der aufgrund des verlorengegangenen Vertrauens der Bürgerinnen und Bürger erlittene Reputationsschaden.

Allein im Zeitraum zwischen Juli 2021 und April 2022 waren nach Recherchen des öffentlich-rechtlichen Mitteldeutschen Rundfunks neun Kommunen in Deutschland von Cyberangriffen getroffen.

Der Aufwand für die Angreifenden sinkt stetig, da immer mehr frei verfügbare Tools für verschiedene Arten von Angriffen im Internet angeboten werden. Waren bisher noch Industrieunternehmen oder größere Kommunalverwaltungen betroffen, ist zu erwarten, dass zukünftig auch Kleinstunternehmen und kleine öffentliche Einrichtungen zum Angriffsziel von Cyberattacken werden. Ebenso werden Schulen in den Fokus von Cyberkriminellen rücken.

Daneben gibt es eine Reihe von Sicherheitsrisiken für die Institution Schule, die nicht auf gezielte Angriffe, sondern auf Ereignisse wie zum Beispiel Brände, Wasserschäden, Naturkatastrophen oder menschliches Versagen zurückzuführen sind (im Anhang werden 47 Elementargefährdungen dargestellt, die vom BSI detektiert wurden). Der Schaden für die Institution Schule, der durch IT-Sicherheitsvorfälle entstehen kann, ist hoch. Schließlich sind diese in der Regel mit Ausfallzeiten, großem Zeitaufwand für Maßnahmen zur Schadensbehebung sowie ungewollten Datenabflüssen verbunden.

Hinzu kommt, dass auf den IT-Systemen der Schulen vor allem personenbezogene Daten Minderjähriger verarbeitet werden, für die ein erhöhtes Schutzniveau gilt.[7]

[6] Cruschwitz, Julia; Haentjes, Carolin, 2022–heute, Hacker-Attacken in Deutschland. IT-Angriffe: Kleine Kommunen, große Gefahr [MDR exakt], https://www.mdr.de/nachrichten/deutschland/gesellschaft/kommune-cyberangriff-it-sicherheit-sachsen-anhalt-thueringen-100.html, abgerufen am 18. November2022.

[7] Dieses Erfordernis wird in „Erwägungsgrund 58“ DSGVO betont.

1.1 Abgrenzung der Bereiche im Kontext der Informationssicherheit

Zum Einstieg in das Thema Informationssicherheit wird in diesem Kapitel zunächst eine Begriffsklärung bezüglich der Informationssicherheit, der IT-Sicherheit und des Datenschutzes dargestellt.

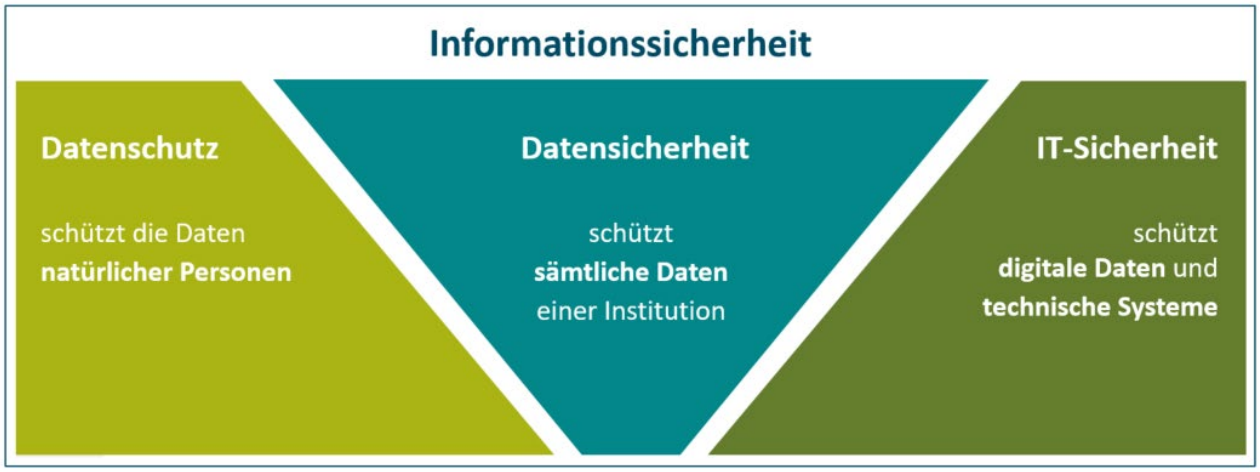

Abbildung 1: Informationssicherheit und ihre Teilbereiche

Informationssicherheit

Die Informationssicherheit umfasst den Schutz sämtlicher Informationswerte in einem Informationsverbund. Der Informationsverbund kann den Schulträger mit den dazugehörigen Schulen beinhalten oder aber nur klar definierte Teilbereiche wie etwa eine Schule. Dies bedeutet, dass zum Beispiel zunächst eine einzelne Schule betrachtet und als Informationsverbund festgelegt wird. Zu einem Informationsverbund gehören alle Objekte, die relevante Teile der Schul-IT sind. Dies sind sowohl (1) Räume inklusive der häuslichen Arbeitsplätze der Mitarbeitenden, (2) IT-Systeme und (3) Netze, zum Beispiel WLAN-Netze, Firewalls und Router, als auch (4) Anwendungen wie Microsoft-Office-Produkte oder die Dateiablage. Informationswerte sind dabei alle Daten in digitaler (Dateien) und analoger Form (z. B. Ausdrucke, handschriftliche Notizen) sowie das Know-how der Mitarbeitenden.

Damit schließt die Informationssicherheit, unabhängig von den Zuständigkeitsbereichen, die Felder Datensicherheit, IT-Sicherheit und einen großen Teil des Datenschutzes ein. Die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität müssen dabei jederzeit eingehalten werden und sind ebenso für alle die Informationssicherheit tangierenden Bereiche gültig.

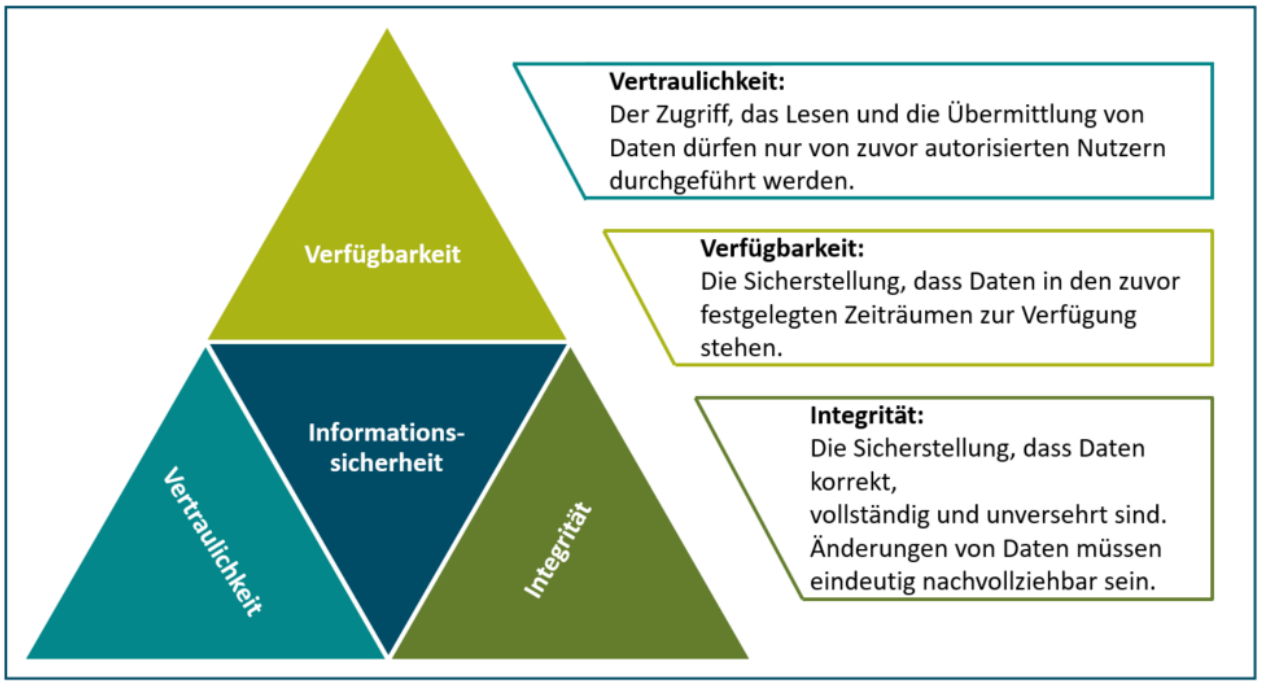

Abbildung 2: Schutzziele der Informationssicherheit

Wie groß der Schutzbedarf eines Objekts ist, hängt jeweils von den potenziellen Schäden ab. Eine genaue Bestimmung ist hier in der Regel nicht möglich. Daher ist es sinnvoll, die möglichen Auswirkungen von Schäden zu kategorisieren. Grundsätzlich bestimmen Sie selbst diese Einteilung. Das BSI schlägt zur Orientierung drei Kategorien vor:

1. Normal: Die Schadensauswirkungen sind begrenzt und überschaubar.
2. Hoch: Die Schadensauswirkungen können beträchtlich sein.
3. Sehr hoch: Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.[8]

Zum gegenwärtigen Zeitpunkt existiert keine allgemeingültige und einheitliche gesetzliche Regelung zum Thema Informationssicherheit in Kommunen. Jedoch gibt es eine Reihe von bundesweiten Regelungen, die nicht unter der Überschrift Informationssicherheit laufen.

IT-Sicherheit

Die IT-Sicherheit umfasst den Schutz von Informationswerten und IT-Systemen unter Einsatz von Informationstechnik. Der Fokus liegt auf dem Schutz sämtlicher elektronisch gespeicherter Informationen und deren Verarbeitung mithilfe technischer Systeme.

Datenschutz

Die unterschiedlichen Datenschutzregelungen des Bundes und der Länder definieren primär den Schutz der personenbezogenen Daten. Dazu wird in vielen Fällen die Frage beantwortet, ob Daten erhoben werden

[8] Bundesamt für Sicherheit in der Informationstechnik [BSI] (2022): https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_4_Schutzbedarfsfeststellung/Lektion_4_01/Lektion_4_01_node.html, abgerufen am 18. November 2022.

dürfen. Im Gegensatz zur Informationssicherheit ist der Datenschutz europaweit in der Datenschutz-Grundverordnung (DSGVO), in landesspezifischen Gesetzen, Richtlinien und Verordnungen sowie in Verwaltungsvorschriften für den schulischen Bereich verankert.

Datensicherheit

Im Gegensatz zum Datenschutz und zur IT-Sicherheit befasst sich das Thema Datensicherheit mit dem generellen Schutz sämtlicher Daten in einer Institution. Die Datensicherheit verfolgt das Ziel, Daten jeglicher Art – neben digitalen Daten auch Ausdrucke und Listen – vor Bedrohungen, Manipulation und unberechtigtem Zugriff zu schützen. Um das zu gewährleisten, werden verschiedene Maßnahmen ergriffen – siehe Kapitel 3.

1.2 Informationssicherheitsrisiken für Schulen

Die Corona-Pandemie hat auch an deutschen Schulen zu einem Entwicklungsschub im Bereich der Digitalisierung geführt. Gleichzeitig haben der „DigitalPakt Schule“ und weitere, länderspezifische Förderprogramme Schulen und Schulträger in die Lage versetzt, den Aufbau leistungsstarker schulischer IT-Netzwerke und die Bereitstellung einer zeitgemäßen digitalen Ausstattung zu beschleunigen.

Daneben kann die Digitalisierung außerdem den Betrieb von Schulserverlösungen erfordern sowie die bedarfsgerechte Beschaffung von mobilen Endgeräten, Anwendungs-Software sowie Präsentationsgeräten und Druckern für Unterrichtszwecke. All diese Komponenten dienen der Informationsverarbeitung für die Schulen. Sie bilden die Grundlage für einen funktionierenden, digital gestützten Unterricht und müssen vor Angriffen und Bedrohungen geschützt werden.

Schulen und Schulträger können Teile der Schul-IT auch auslagern. Dafür bieten sich Cloud-Lösungen oder die Unterstützung durch externe Dienstleister an. Dies verringert die Komplexität der Anforderungen an die Informationssicherheit, die von der Schule beziehungsweise dem Schulträger gegebenenfalls verantwortet werden muss.

Gefährdungen[9] können dazu führen, dass die Schutzziele nicht eingehalten werden können. Beispiele:

- Vertraulichkeit
  - Benotungen von Schülerinnen und Schülern sind für nicht Berechtigte einsehbar
  - Ausdrucke liegen auf dem Kopierer und können von nicht Berechtigten gelesen oder verbreitet werden
  - Passwörter werden auf Listen verteilt und sind für alle Schülerinnen und Schüler der Lerngruppe einsehbar
- Verfügbarkeit
  - Der Server fällt aus und somit stehen die Unterlagen für das Lehren und Lernen nicht zur Verfügung
  - Das Internet ist nicht verfügbar
  - Räume können nicht betreten werden – der Unterricht muss ausfallen
- Integrität
  - Dokumente wurden verändert und entsprechen nicht mehr dem Original

[9] Zur Unterscheidung zwischen Gefährdung, Bedrohung und Schwachstelle siehe Glossar.

- Passwörter für Geräte stimmen nicht

Die Konsequenz daraus ist in den meisten Fällen, dass der Schulbetrieb nicht mehr reibungslos funktioniert.

Ein Informationssicherheitsmanagementsystem (ISMS) ist daher auch für Schulen und Schulträger mittelfristig unabdingbar.

Bei vielen Schulträgern und Schulen ist das Thema der Informationssicherheit bereits in den Fokus gerückt. So wird zeitgleich mit dem Auf- und Ausbau der schulischen Digitalausstattung die Einrichtung grundlegender technischer Schutzmechanismen (Firewalls und sichere Netzwerkkonzepte) heute bereits vielfach mitgedacht und umgesetzt.

Die zunehmende Zahl an Cyberangriffen in der jüngsten Vergangenheit zeigt aber, dass der professionelle Betrieb der IT-Infrastruktur viele Schulen und Schulträger weiterhin vor große Herausforderungen stellt. Vielfach fehlt es sowohl an konzipierten und dokumentierten Vorsorgemaßnahmen für IT-Sicherheitsnotfälle als auch an Strukturen, Prozessen und klar definierten Zuständigkeiten für ein sicheres Handeln in Notfallsituationen.

Darüber hinaus sind aber auch die Herausforderungen durch den Schulbetrieb an sich zu regeln: zum Beispiel im Fall der mobilen Endgeräte für die Schülerinnen und Schüler, die teilweise per GYOD („Get your own device“) oder BYOD („Bring your own device“) in das IT-Netzwerk eingebunden werden, jedoch aufgrund eines bestimmten Finanzierungsmodells auch privat genutzt werden können. Ebenso schwierig verhält es sich mit den mobilen Endgeräten der Lehrkräfte, die zum Teil deren Privateigentum sind und von denen wiederum Unterrichtsmaterialien per USB-Stick auf die Schulcomputer übertragen werden.

Des Weiteren sind auch Daten, die auf Papier zur Verfügung stehen, wie zum Beispiel in Klassenbüchern oder auf Teilnahmelisten, Informationen, die für den Schulalltag notwendig sind, aber geschützt werden müssen.

Nicht zuletzt ist auch das Know-how der Lehrkräfte und der Mitarbeitenden der Schulen zu berücksichtigen. Verfügt zum Beispiel nur eine Person über das Wissen bezüglich der Zugangsdaten oder der Berechtigungen, ist das eine Schwachstelle, da bei einem Ausfall dieser Person das benötigte Wissen fehlt.

In diesem Sinne sollen die vorliegende Handreichung und die dazugehörigen Quick-Check-Bögen den Einstieg in das Thema ermöglichen sowie konkrete Maßnahmen und Schritte zur Erreichung einer Basis-Absicherung der Schul-IT nach BSI-Grundschutz aufzeigen.

2 Schulträgertypen und Betriebsstrukturen

Im vorliegenden Kapitel werden zunächst die unterschiedlichen Schulträgertypen in der Bundesrepublik Deutschland beleuchtet und zentrale kommunale Strukturen, die am Aufbau und dem Betrieb des Informationssicherheitsmanagements in der Schul-IT beteiligt sind, erläutert. Danach wird ein Überblick über die zentralen Rollen und Verantwortlichkeiten gegeben.

2.1 Schulträgertypen und IT-Steuerung in Kommunen und kommunaler Struktur

In den Verantwortungsbereich der öffentlichen Verwaltung in der Bundesrepublik Deutschland gehört die Informations- und Kommunikationstechnik (IKT). Durch sie soll gewährleistet werden, dass staatliche Institutionen mit einer zeitgemäßen IT-Infrastruktur ausgestattet sind. Dazu zählt auch die zeitgemäße Ausstattung von öffentlichen Schulen. Damit fallen der Aufbau und die Steuerung der Schul-IT derzeit bundesweit in den Verantwortungsbereich der kommunalen Schulträger.

Allerdings sehen sich die Schulträger von Bundesland zu Bundesland, gemäß den dort jeweils geltenden Schulgesetzen und kommunalen Vorgaben, unterschiedlichen rechtlichen Rahmenbedingungen gegenüber. Diese wirken sich wiederum auf die Verwaltung der Schul-IT aus. Die rechtlichen Rahmenbedingungen sind sowohl für die Schulträger in öffentlicher als auch die in freier Trägerschaft bindend.[10]

Die meisten Schulgesetze enthalten bislang aber kaum Vorgaben dazu, wie mit dem Thema Informationssicherheit umzugehen ist. Die Schulträger sind hier auf Handreichungen und Anleitungen, wie etwa das BSI-IT-Grundschutz-Kompendium, angewiesen, die aber oft nicht auf die speziellen Gegebenheiten der Schul-IT eingehen.

Auch die Sicherstellung und die Überwachung der Einhaltung von Informationssicherheitsanforderungen sind derzeit nicht oder kaum zu gewährleisten, da bereits die Umsetzung von der personellen Kapazität und der technischen Ausstattung des jeweiligen Schulträgers abhängig ist.

Je nach Größe des Schulträgers unterscheiden sich die IT-Verantwortlichkeiten und die -Strukturen deutschlandweit sehr stark. Während in strukturärmeren Gegenden einzelne Schulen die Schul-IT zumeist in Eigenverantwortung betreiben, ist eine zentral verwaltete und organisierte Schul-IT-Landschaft in großen Städten oder Landkreisen keine Seltenheit mehr. Die folgende Übersicht zeigt beispielhaft einen Vergleich der organisatorischen und strukturellen Gegebenheiten von vier verschiedenen Schulträgertypen:

Tabelle 1: Steuerung durch verschiedene Schulträgertypen (die Unterschiede beruhen auf Erfahrungen aus der Beratung von verschiedenen Schulträgern und Kommunen durch die PD)

Schulträgertyp	Charakteristika
Typ 1 – Gemeinde, kreisangehörige Stadt	— Mehrheitlich Grundschulen in der Trägerschaft (zum Teil auch weiterführende Schulen) — Die schulische IT wird, wenn überhaupt vorhanden, meistens durch eine kleine IT-Abteilung beim Schulträger gesteuert
Typ 2 – Schulträgerverbund	— Mehrheitlich Grundschulen und nur wenige weiterführende Schulen in der Trägerschaft — Zusammenschluss aus mehreren Schulträgern

[10] siehe Anhang: Schulgesetzgebung der Bundesländer.

Schulträgertyp	Charakteristika
	— Eine gebündelte Schul-IT-Abteilung ist beim Schulträgerverbund meist (noch) nicht vorhanden
Typ 3 – kreisfreie Stadt	— Meist sind alle Schulformen in der Trägerschaft vertreten — Die schulische IT wird von einer internen IT-Abteilung, gegebenenfalls unter Einbindung einzelner oder mehrerer IT-Dienstleister der Stadt, gesteuert
Typ 4 – Landkreis	— In manchen Landkreisen sind alle Schulformen vertreten, meist aber vorwiegend weiterführende Schulen, berufsbildende Schulen und Förderschulen — Die schulische IT wird mehrheitlich vom Landkreis gesteuert.

Die hier dargestellten Schulträgertypen unterscheiden sich also vor allem im Hinblick auf das Ausmaß an Zentralisierung und Standardisierung der IT-Landschaft und des IT-Betriebs. Eine Zentralisierung und Standardisierung bringen für die Schulträger eine Reihe von Vorteilen, da die notwendigen Prozesse effizienter und ressourcenschonender aufgebaut werden können.

2.2 Zentrale Rollen und Verantwortlichkeiten bei der Steuerung der Schul-IT

Ein wesentliches Element zur Einführung eines Informationssicherheitsmanagements gemäß dem BSI-Grundschutz-Kompendium ist die klare Zuweisung von Rollen und Verantwortlichkeiten. Durch die entsprechenden Stellenbeschreibungen wird festgelegt, wo welche Entscheidungen getroffen werden, welche Rollen es im IT-Organigramm gibt und welche Verantwortlichkeiten den einzelnen Personen zugewiesen sind.

In der folgenden Übersicht werden die wichtigsten Rollen und Verantwortlichkeiten im Bereich der Schul-IT dargestellt. Die im Rahmen dieser Handreichung ausgesprochenen Empfehlungen sind nur auf öffentliche Schulträger ausgerichtet.

Tabelle 2: Relevante Rollen und Verantwortlichkeiten für die Steuerung der Schul-IT

Rollenbezeichnung	Verantwortlichkeit
Verwaltungsvorstand (Landrätin/Landrat, Oberbürgermeisterin/Oberbürgermeister, Bürgermeisterin/Bürgermeister)	Trägt die organisatorische Verantwortung einer Gemeinde, Kommune oder Stadt und die Gesamtverantwortung für die Informationssicherheit
IT-Leiterin/-Leiter (der Schul-IT)	Verantwortet, dass im IT-Betrieb alle erforderlichen Maßnahmen umgesetzt werden
Schulische/r IT-Administratorin/-Administrator, IT-Koordinatorin/-Koordinator	Verantwortet den IT-Betrieb in den schulischen Liegenschaften mit Administratorenrechten
Mitarbeitende der Beschaffungsstellen/Vergabestellen	Prüfen, ob Kriterien der Informationssicherheit in den Vergabeunterlagen abgefragt werden
Mitarbeitende aus dem Schulverwaltungsbereich (Schule/Schulträger)	Definieren und prüfen konsultierend, ob die Auflagen der Informationssicherheit in den Schulen eingehalten werden, und sie besitzen Zugangsrechte zu den Systemen (nur zu Informationszwecken)

Rollenbezeichnung	Verantwortlichkeit
Städtische IT-Mitarbeitende oder gegebenenfalls IT-Mitarbeitende für Schul-IT	Verantworten den Betrieb der IT-Infrastruktur in den städtischen Liegenschaften und von Heim-Arbeitsplätzen mit Administratorenrechten und setzen die Informationssicherheitsrichtlinien um
Externe IT-Dienstleister – kommunal und privatwirtschaftlich	Zusammenschlüsse nach den Regeln kommunaler Zusammenarbeit oder wirtschaftlich ausgerichtete Einheiten, die über IT-Expertise verfügen und gegebenenfalls eingeschränkte Administratorenrechte erhalten; unterstehen den Informationssicherheits- und Datenschutzregelungen des Schulträgers
Medienbeauftragte	Bilden die Schnittstelle zwischen dem Kollegium, dem „Supportteam“ des Schulträgers und den Fachberatenden am staatlichen Schulamt mit deren Beratungsteams
Informationssicherheitsbeauftragte (ISB)	Prüfen, ob die zur Einhaltung der Informationssicherheit notwendigen Anforderungen erfüllt werden
Datenschutzbeauftragte (DSB)	Übernehmen Unterrichtung, Beratung des Verantwortlichen und Überwachung der Einhaltung der Verordnungen und anderer Datenschutzvorschriften

Neben diesen zentralen Rollen sind für die Informationssicherheit immer auch alle anderen Mitarbeitenden im Informationsverbund von großer Bedeutung. Sie sind es, die die Anforderungen des Informationssicherheitsmanagements umsetzen müssen, und ihre Wachsamkeit entscheidet oft über den Erfolg oder Misserfolg eines Angriffes. Die fortlaufende Schulung und die Sensibilisierung der eigenen Mitarbeitenden sind daher ein wichtiger Teil des Informationssicherheitsmanagements – das BSI stellt hierfür hilfreiche Informationen zur Verfügung[11].

Im Rahmen der Schul-IT bezieht der benannte Personenkreis nicht nur die Mitarbeitenden in der Schulverwaltung ein, sondern die Gesamtheit des pädagogischen Personals sowie Hausmeisterinnen und Hausmeister und alle anderen Personen mit Zutritt zu den Schulbehörden und Schulgebäuden. Gegebenenfalls haben sie Zutritt zu den IT-Systemen.

Daneben sind auch Eltern, Schülerinnen und Schüler wichtig für den Erfolg des Informationssicherheitsmanagements. Hier muss eine Regelung dazu geschaffen werden, welche Rolle die Sensibilisierung des pädagogischen Personals, der Eltern, Schülerinnen und Schüler einnimmt. Gerade der verstärkte Einsatz von mobilen Endgeräten, die einen Zugriff auf Server, Netzwerke und damit auf sensible Daten zulassen, erfordert einen verantwortungsvollen Umgang mit Zugangsdaten und die Achtsamkeit aller Beteiligten. Zentrale Anforderungen zur Sensibilisierung der Mitarbeitenden, Nutzerinnen und Nutzer finden sich in dem Quick-Check_02 „Sensibilisierung“.

2.3 Vereinfachter Netzwerkplan

Eine Übersicht über die Netzwerkkomponenten bieten Netzwerkpläne. Diese beinhalten alle IT-Dienste und IT-Infrastrukturen. Eine Darstellung von verschiedenen möglichen Netzwerkplänen für Schul-IT finden Sie in der Handreichung „Informationssicherheit Schule im IT-Betrieb: Erste Schritte“, welche im Jahr 2023 verfügbar sein wird.

[11] Bundesamt für Sicherheit in der Informationstechnik [BSI] (2022b): Awareness, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Faktor-Mensch/Awareness/awareness_node.html, abgerufen am 18. November 2022.

Im folgenden Beispiel-Netzwerkplan wird dargestellt, wie ein gut gepflegter Plan einen Überblick über alle relevanten IT-Komponenten geben kann. Darüber hinaus dient er als Grundlage für die Erarbeitung der verschiedenen Konzepte (CON) zur Informationssicherheit: Er verdeutlicht, welche IT-Komponenten geschützt werden müssen, und hilft dabei, abzuleiten, welche Nutzerinnen und Nutzer auf welche Bereiche des Netzes Zugriff haben.

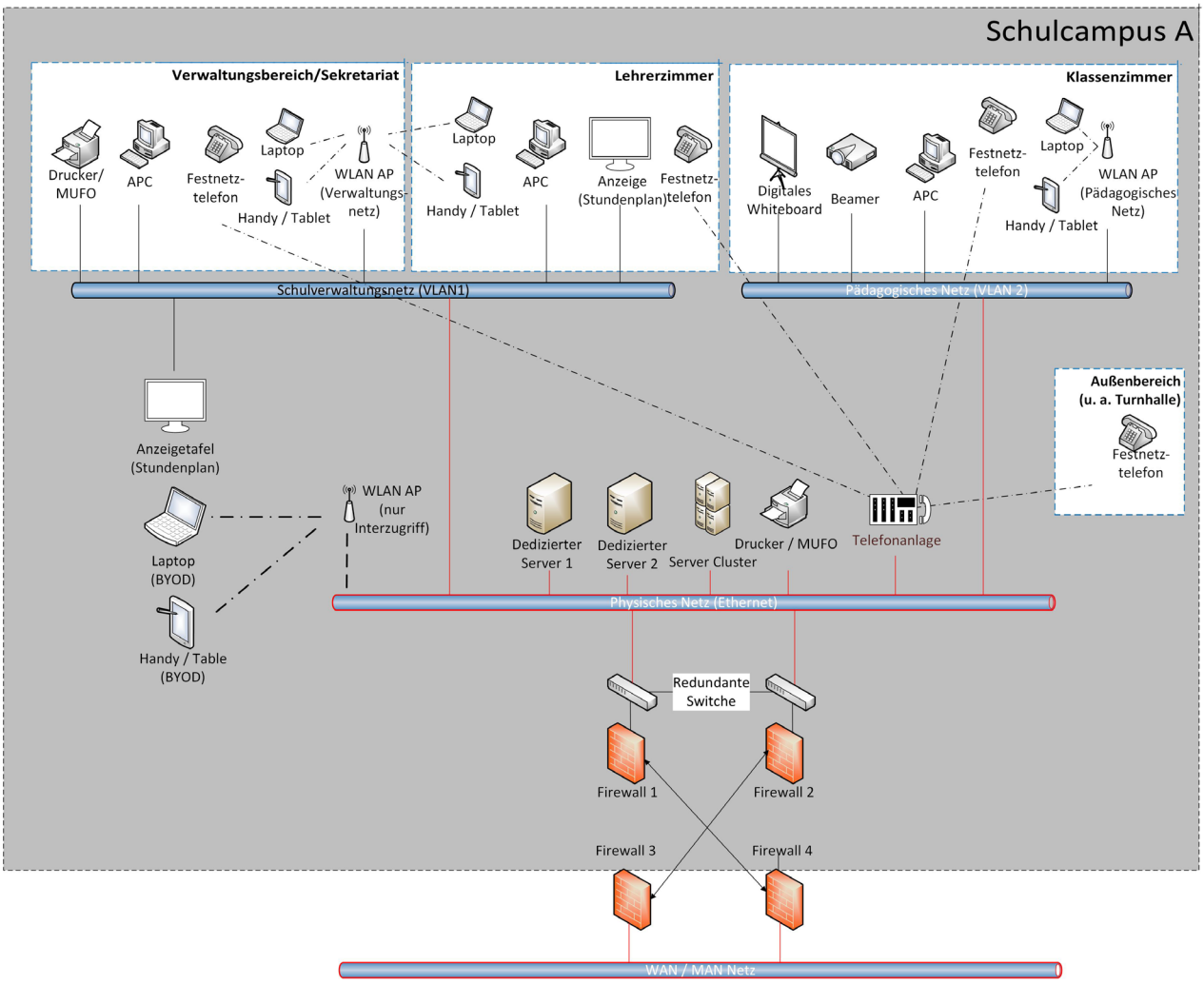

Abbildung 3: Beispiel Netzwerkplan

3 Informationssicherheit für Schulträger und Schulen

Es mag im ersten Moment überraschen, aber Informationssicherheit ist in erster Linie eine organisatorische Aufgabe und erst in zweiter Linie ein technisches Thema.

Ausschlaggebend ist eine systematische Integration von Informationssicherheit in das jeweilige Informationssicherheitsmanagement von Kommunen und Schulen. Die wohl wichtigste Ressource sind dabei die Mitarbeitenden der Schule und der Schulträger sowie gegebenenfalls involvierte Dienstleister.

Für die Umsetzung des Informationssicherheitsmanagements stehen Schulträgern und Schulen verschiedene Normen zur Verfügung, an denen sie sich orientieren können: International hat sich die *Norm ISO 27001* etabliert. Im deutschen Kontext ist darüber hinaus das auf der ISO (Internationale Organisation für Normung) basierende *IT-Grundschutz-Kompendium* des BSI zum Standard für Informationssicherheit geworden.

Weitere Standards sind C*ISIS 12* und *VdS 1000*. Das BSI-Grundschutz-Kompendium[12] definiert dabei zentrale Risiken und elementare Gefährdungen und formuliert standardisierte Anforderungen in den Bereichen Organisation, Personal, Infrastruktur und Technik, um diese Risiken und Gefährdungen abzuwenden. Das Grundschutz-Kompendium des BSI stellt damit für Schulträger und Schulen einen möglichen Rahmen dar, um sich einerseits dem Thema Informationssicherheit nähern und um andererseits Gefährdungslagen ihres Informationsverbunds einzuschätzen und präventive Maßnahmen gegen sie ergreifen zu können.

Im Kern des IT-Grundschutz-Kompendiums stehen Bausteine, die in **Prozess- und Systembausteine** unterteilt sind. Jeder Baustein bezieht sich auf bestimmte Zielobjekte und die jeweils relevanten Risiken und Gefährdungen für diese Objekte. Die Zielobjekte sind je Baustein unterschiedlich. Manchmal zielen sie auf Prozesse ab (z. B. die Einrichtung von Sicherheitsmanagementstrukturen), manchmal auf technische Komponenten (z. B. Firewall) oder auf Gebäude (z. B. Serverräume). Jeder Baustein stellt zentrale Anforderungen sowie Rollen vor, welche erfüllt sein müssen, um den Gefährdungen adäquat begegnen zu können. Die Anforderungen gliedern sich dabei auf drei Ebenen: Basisanforderungen, Standardanforderungen und Anforderungen bei erhöhtem Schutzbedarf. **Basis- und Standardanforderungen** sind auf den normalen Schutzbedarf ausgerichtet, wobei die Basisanforderungen stets vorrangig umgesetzt werden sollten, da sie mit dem geringsten Aufwand den größten Nutzen erzielen und für die erfolgreiche Implementierung des jeweiligen Bausteins zentrale Elemente behandeln.

Wenn die Basisabsicherung erfolgreich umgesetzt ist und alle zentralen Prozesse und Komponenten in das Informationssicherheitsmanagement (ISMS) aufgenommen sind, empfiehlt es sich, in einem nächsten Schritt die Standard-Anforderungen anzugehen.

Für eine schnelle Orientierung im Bereich der kommunalen IT hat die Arbeitsgruppe Kommunale Basis-Absicherung [AG KOBA] darüber hinaus einen Leitfaden herausgegeben, in welchem die „Mindestsicherheitsmaßnahmen, die in einer Kommunalverwaltung umzusetzen sind, um sich nach hiesiger Einschätzung nicht der groben Fahrlässigkeit schuldig zu machen“[13], definiert sind. Diese Handreichung basiert auf dem

[12] Bundesamt für Sicherheit in der Informationstechnik [BSI] (2023): IT-Grundschutz-Kompendium, Reguvis Fachmedien GmbH, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4#download=1, abgerufen am 07. Februar 2023.

[13] Arbeitsgruppe Kommunale Basis-Absicherung [AG KOBA] (2022): IT-Grundschutz-Profil Basis-Absicherung Kommunalverwaltung, S. 3, https://www.landkreistag.de/images/stories/themen/egovernment/220331_IT-Grundschutz-Profil.pdf, abgerufen am 23. November 2022.

BSI-Standard 200-2 und bietet einen schnellen Einstieg in das Thema Informationssicherheit. Das angestrebte Schutzniveau entspricht dabei der BSI-Basis-Absicherung. Dementsprechend werden die Basisanforderungen als zentral hervorgehoben. Teilweise enthalten die Empfehlungen aber auch Anforderungen des Standard- oder erhöhten Schutzniveaus, um den spezifischen Herausforderungen der Kommunen zu begegnen. Das Papier stellt dabei nur einen Einstieg in die Thematik dar und skizziert bereits als mittelfristiges Ziel die Standardabsicherung: „Ziel muss es sein, darauf aufbauend mittelfristig ein Sicherheitskonzept gemäß der Standard-Absicherung (definiert in [BSI-200-2]) zu erstellen, da nur dies dem Schutzbedarf der Daten und Prozesse einer Kommunalverwaltung gerecht wird.“[14]

Im Folgenden werden zunächst konkrete, zentrale Empfehlungen zur Umsetzung des Informationssicherheitsmanagements bei Schulträger und Schulen gegeben. Dieser Überblick erleichtert den Einstieg in die Thematik und bietet eine Orientierung für mögliche Vorgehensweisen bei der Umsetzung. Im Anschluss wird ein Überblick über das BSI-Grundschutz-Kompendium und seine dazugehörigen Schichten und Bausteine gegeben. Diese Übersicht ersetzt nicht die genaue Lektüre des BSI-Grundschutz-Kompendiums, bietet aber einen ersten Einblick und Zusammenfassung. Leser und Leserinnen, die mit den Bausteinen und den Anforderungen bereits vertraut sind, können nach eigenem Ermessen mit Kapitel 4 fortfahren.

3.1 Umsetzung von Informationssicherheit bei Schulträgern und Schulen

Für Schulträger und Schulen stellt sich zu Beginn die Frage, wie die Umsetzung der Informationssicherheitsmanagements am besten initiiert werden kann. Die Liste der Gefahren ist lang und die umzusetzenden Anforderungen und Maßnahmen erscheinen oft komplex und vielfältig. Tatsächlich kann aber schon ein erster Check helfen zu erkennen, welchen Schutzbedarf die eigene Institution hat, an welcher Stelle sie im Moment steht und welche wenige erste Schritte helfen können, die Informationssicherheit zu erhöhen. Bevor in Kapitel 3.2 ein Überblick über die Bausteine des BSI gegeben wird, soll hier ein Überblick über mögliche Ansätze zur Umsetzung der Informationssicherheit bei Schulträgern und Schulen gegeben werden.

Es ist ratsam, die Anforderungen der Basis-Absicherung als erstes umzusetzen, da sich auf diese Weise mit wenig Aufwand bereits eine grundlegende Informationssicherheit erreichen lässt. Vielfach sind gerade in diesem Bereich viele Dinge bereits gegeben oder sind leicht umzusetzen. So existiert häufig schon eine Regelung der Accounts von Nutzerinnen und Nutzern, eine Passwortvergabe sowie eine grundlegende Übersicht vorhandener IT-Infrastruktur und Geräteanbindung. Ebenso ist zumeist schon verantwortliches und verwaltendes Personal auf einige Themenbereiche verteilt und zugewiesen worden. Auf diese vorhandenen Informationen kann mit Hilfe der vorliegenden Handreichung und der dazugehörigen Quick-Checks angeknüpft und die Basisabsicherung hergestellt werden. Eine ausführliche Risikoanalyse ist im Bereich der Basisabsicherung noch nicht nötig. Dennoch empfiehlt es sich direkt zu Anfang einen umfassenden Überblick über die zu schützenden Zielobjekte des Informationsverbundes zu machen und Risiken und Gefährdungen für jedes Zielobjekt zu betrachten.

[14] Arbeitsgruppe Kommunale Basis-Absicherung [AG KOBA] (2022): IT-Grundschutz-Profil Basis-Absicherung Kommunalverwaltung, S. 4, https://www.landkreistag.de/images/stories/themen/egovernment/220331_IT-Grundschutz-Profil.pdf, abgerufen am 23. November 2022.

Generell lassen sich zwei grundsätzliche Ansätze für den Einstieg in den systematischen Aufbau von Informationssicherheit unterscheiden:

Ansatz 1: Basis-Absicherung nach BSI

Bei diesem Ansatz werden erste systematische Schritte und Maßnahmen zur Erreichung einer Basis-Absicherung und Etablierung erster organisatorischer Veränderungen zur grundlegenden Verankerung von Informationssicherheit in der Schulverwaltung und den einzelnen Schulen angestrebt. Die Handreichung in Verbindung mit den Quickchecks bieten eine gute Grundlage, um die Testierung vorzubereiten. In der Praxis hat sich eine Zeitspanne von ca. 2 Jahren für die Vorbereitung der Testierung gezeigt.

Ansatz 2: Zertifizierung nach BSI oder ISO 27001

Es wird von Anfang an ein umfassender, langfristiger Ansatz mit dem Ziel einer tiefgreifenden Verankerung des Themas Informationssicherheit in der Schulverwaltung und Schule sowie permanenten Weiterentwicklung verfolgt. Eine Zertifizierung nach BSI oder ISO 27001 sowie eine regelmäßigen Re-Zertifizierung durch unabhängige Audits wird dabei angestrebt. Auch hier kann mit einer Zeitspanne von bis zu zwei Jahren gerechnet werden.

Für die Mehrheit der Schulträger und Schulen empfiehlt sich vermutlich zunächst Ansatz 1 als niedrigschwelliger Einstieg in das komplexe Thema Informationssicherheit. Dabei stehen die Umsetzung wesentlicher Aspekte eines Informationssicherheitsmanagementsystems (ISMS) und dafür notwendiger organisatorischer wie technischer Maßnahmen für ein mögliches Testat zur Basis-Absicherung nach BSI-IT-Grundschutz-Kompendium im Vordergrund. Die vorliegende Handreichung fokussiert auf diesen Ansatz. Ziel ist es dabei, Schulträgern und Schulen in einem überschaubaren Zeitraum substanzielle Verbesserungen bei der Informationssicherheit zu ermöglichen und mit dem Aufbau eines Informationssicherheitsmanagementsystems zu beginnen.

Allerdings kann dieser kleine Ansatz für eine vollständige Absicherung nicht dauerhaft für sich alleine stehen, sondern muss lang- und mittelfristig um den indes eigenständigen Ansatz 2 ergänzt werden. So kann ein umfassendes und systematisches Informationssicherheitsmanagement etabliert werden. Nur so werden eine permanente Anpassung und eine stetige Qualitätssicherung gewährleistet.

Ansatz 2 bietet Schulträgern und Schulen auch die Möglichkeit, eine Zertifizierung gemäß dem BSI-IT-Grundschutz (Kern- oder Standardabsicherung) oder gemäß der internationalen Norm ISO 27001 zu erreichen. Tatsächlich kann es jedoch aus wirtschaftlichen Gründen vorkommen, dass eine solche Zertifizierung nicht oder für einen längeren Zeitraum nicht möglich ist. In diesem Fall sollte trotzdem ein umfassender Schutz angestrebt und sollten die Umsetzung der notwendigen Maßnahmen sowie die Erfüllung der Kriterien intern überwacht werden.

Unabhängig vom „Ziel-Standard“ sollten Schulen und Schulträger also das Informationssicherheitsmanagement als zentrale Aufgabe in der Schul-IT verankern, auch wenn das Ziel einer Zertifizierung und das damit verbundene Audit-Verfahren unter Umständen erst mittelfristig, nach mehreren Jahren erreicht werden können. Abbildung 4 zeigt beispielhaft das Vorgehen zur Umsetzung der Informationssicherheitsanforderungen sowie der anschließenden Auditierung und Testierung, wie sie sich aus Ansatz 2 ergeben würde.

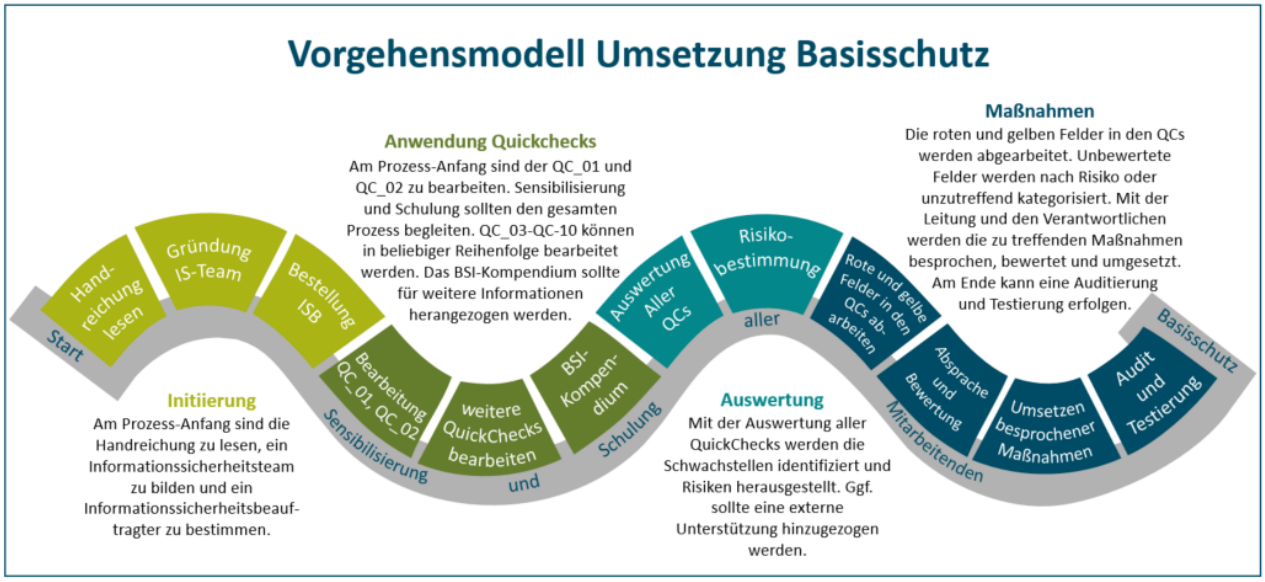

Abbildung 4: Prozess zur Umsetzung des Informationssicherheitsmanagement

Um die Umsetzung von Ansatz 1 für den Informationsverbund einzuleiten, bietet die vorliegende Handreichung eine Reihe von Testbögen, sogenannte Quick-Checks an, mit deren Hilfe Sie den Ist-Stand Ihrer Prozesse und Komponenten erfassen, offene „Baustellen“ identifiziere und beginnen können, erste Maßnahmen zu planen. Die Quick-Checks orientieren sich an den Bausteinen des BSI-Grundschutz-Kompendiums, die im Abschnitt 3.2 übergreifend dargestellt sind. Abbildung 5 zeigt beispielhaft das Vorgehen zur Einführung eines Informationssicherheitsmanagementsystems mit Hilfe der Quick-Checks.

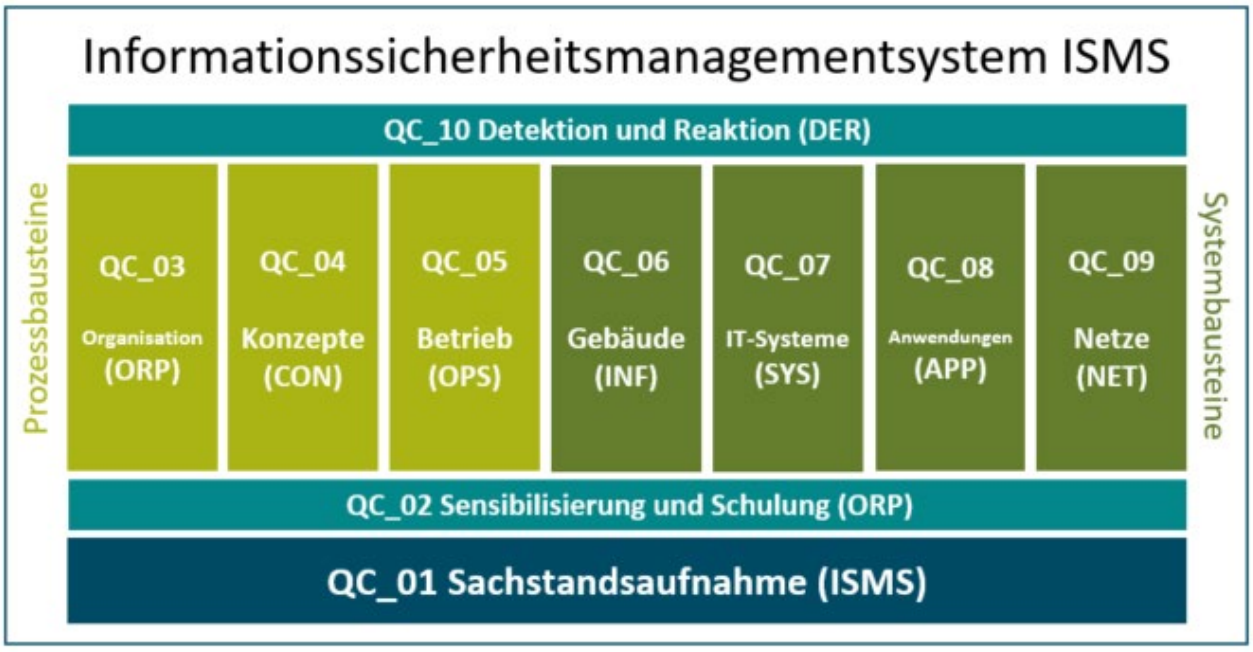

Abbildung 5: Einführung eines Informationssicherheitsmanagementsystems mithilfe der Quick-Checks (Quelle: SiKoSH, BSI-Grundschutz-Kompendium, angepasst)

Im ersten Prozessschritt (Initiierung) wird eine verantwortliche Person für das Thema Informationssicherheit benannt. Zudem wird eine Arbeitsgruppe mit Vertreterinnen und Vertretern der Schulen (Medienbe-

auftragte / IT-Koordinatorinnen u. -Koordinatoren) und des Schulträgers (Abteilungsleitung Schulverwaltung, Verantwortliche für Schul-IT) zur Umsetzung der weiteren Prozessschritte installiert. Der Quick-Check „QC_01 Sachstandsaufnahme (ISMS)“ (siehe Anhang) bietet für die hier benannten organisatorischen Schritte eine grundlegende Orientierung und ein Fragenset zur Sachstandserhebung.

Neben der Klärung von Verantwortlichkeiten werden bereits zu Beginn der Umsetzung die Sicherheitsprozesse in der Organisation verankert, ein Berichts- und Dokumentationswesen fixiert sowie Optimierungen der Informationssicherheit überprüft und geplant.

Die Sensibilisierung und die Schulung der Mitarbeitenden (QC_02 Sensibilisierung (ORP) bilden neben der Sachstandsaufnahme die Basis zur Umsetzung der Informationssicherheitsaufgaben.

Nach dem Prüfen und Umsetzen der Fundamente der Informationssicherheit können die weiteren Quick-Checks in beliebiger Reihenfolge bearbeitet werden, wobei jedoch auf Vollständigkeit zu achten ist.

Sollten Sie eine Zertifizierung Ihrer Basisabsicherung anstreben, ist es ratsam, das *IT-Grundschutzkompendium* noch einmal im Detail durchzugehen, da in den Quick-Checks die Inhalte des BSI zugunsten eines schnelleren Überblicks zusammengefasst und teilweise verallgemeinert wurden.

3.2 Die Bausteine zum Informationssicherheitsmanagements nach BSI-IT-Grundschutz

Insgesamt umfasst das BSI-Grundschutz-Kompendium Prozess- und Systembausteine. Jeder Baustein zielt auf den Schutz bestimmter Komponenten oder Prozesse ab. Die Bausteine werden im BSI noch einmal in thematische Schichten gruppiert, wobei jede Schicht weitere Teilschichten enthalten kann. So gehören zur Schicht „ORP: Organisation und Personal“ alle Bausteine, die sich um personelle und organisatorische Sicherheitsaspekte drehen.

Zur Orientierung sind die einzelnen Anforderungen in jeder Schicht jeweils mit einer Kombination aus Buchstaben und Ziffern gekennzeichnet. So ist der erste Baustein mit dem Namen „Organisation“ in der Schicht „ORP“ mit „ORP.1“ beziffert. Die erste Anforderung „Festlegung von Verantwortlichkeiten und Regelungen“ in diesem Baustein trägt dann das Kürzel „ORP.1.A1“, die zweite Anforderung „ORP.1.A2“ und so weiter.

Im vorliegenden Kapitel erhalten Sie einen Überblick über die Schutzanforderungen der verschiedenen Schichten an die Prozess- und Systembausteine sowie eine Erläuterung zu deren Bedeutung für den Arbeitsbereich Schul-IT.

Der Fokus des Kapitels liegt auf der Basisanforderung des BSI. Die zentralen Anforderungen der Schichten sind jeweils am Anfang in einem petrolfarbenen Kästchen zusammengefasst. Ein farblich hervorgehobener Kasten verlinkt auf die entsprechenden Quick-Checks. Die Zusammenfassung der Bausteine in der jeweiligen Schicht erfolgt in einer Beschreibung. Zentrale Rollen und Begriffe werden teilweise in einem weiteren blauen Kasten erklärt.

Da die Schul-IT eine Teilmenge der kommunalen IT darstellt und IT-Infrastrukturen eng miteinander verzahnt sind, bezieht sich diese Handreichung auch auf die Empfehlungen des *IT-Grundschutzprofils Basis-Absicherung Kommunalverwaltung*. Dabei identifiziert das IT-Grundschutzprofil einzelne Bausteine einer Schicht als besonders relevant und gibt darüber hinaus weiterführende Hinweise und Empfehlungen. Die hervorgehobenen Bausteine und eine Zusammenfassung der Empfehlungen werden jeweils unter der Zusammenfassung der Schicht dargestellt.

3.2.1 Die Schichten der Prozessbausteine im BSI

ISMS – Sicherheitsmanagement

Diese Schicht ist für Schulträger zentral, da sie sicherstellt, dass ein Managementsystem aufgebaut und betrieben wird sowie die erforderlichen Konzepte festgelegt, Leitlinien erarbeitet und Informationsflüsse etabliert werden.

Zentrale Aufgaben

— Eine/einen Verantwortliche/n für die IT-Sicherheit benennen, die/der das Thema in die Hand nimmt.

Quick-Check 01 ISMS

Besonders zentral ist die Festlegung von Personen, die das Thema Informationssicherheit in der Schul-IT intensiv vorantreiben. Durch die Trennung der äußeren und inneren Schulangelegenheiten ergibt sich in diesem Feld eine Herausforderung, da die Verantwortung für die Informationssicherheit – je nach Regelungen des Bundeslandes – bei der Schulleitung oder beim Schulträger liegen kann. Aus diesem Grund ist es sinnvoll, zunächst die entsprechenden Festlegungen zu prüfen.

Generell ist zu empfehlen, dass Vertreterinnen und Vertreter der Schulen und des Schulträgers ein Informationssicherheitsteam aufstellen, das die Informationssicherheit unabhängig von der Verantwortung für diese vorantreibt.

Diese Schicht beinhaltet nur einen Baustein („ISMS.1“). Folglich ist der Baustein gemäß dem BSI-Grundschutz-Kompendium und dem IT-Grundschutzprofil Basis-Absicherung Kommunalverwaltung auf die ganze Organisation anzuwenden.

Beschreibung der Schicht „(Informations-) Sicherheitsmanagement“

Diese Schicht beinhaltet nur einen Baustein. Dieser beschreibt die Notwendigkeit, dass ein funktionierendes Managementsystem für Informationssicherheit (ISMS) eingerichtet ist und alle Planungs-, Lenkungs- und Kontrollaufgaben durchgeführt werden, die für die Herstellung von Informationssicherheit wichtig sind. Das Sicherheitsmanagement muss dabei in die gesamte Struktur des Informationsverbundes eingebettet sein.

Der Baustein baut auf den BSI-Standards 200-1 „Managementsysteme für Informationssicherheit“ und 200-2 „IT-Grundschutz-Methodik“ auf und fasst daraus die wichtigsten Aspekte zum Sicherheitsmanagement zusammen. Der Baustein greift auf die Schicht „DER“ (insb. Baustein „DER 3.1.“) und „ORP“ (insb. Bausteine „ORP.1“, „ORP.2“ und „ORP.3“ zu).

Die größten Gefahren für die erfolgreiche Umsetzung des Bausteins sind fehlende Investitionen und fehlende Aktualität sowie mangelndes Durchsetzungsvermögen, nicht vorhandenes Verantwortungsgefühl und nicht geklärte Zuständigkeiten. Gesetzliche Vorgaben sind unbedingt einzuhalten.[15]

Basisanforderungen:

— Ziele, Leitlinie und Konzeptrahmen festlegen
— Informationssicherheitsbeauftragte bestimmen
— Organisationsstrukturen schaffen und die Informationssicherheit in organisationsweite Abläufe und Prozesse inkludieren
— Sicherheitsmaßnahmen festlegen
— Mitarbeitende in den Prozess inkludieren

[15] Siehe beispielsweise das Sächsisches Informationssicherheitsgesetz [SächsGVBl.], S. 630, https://www.revosax.sachsen.de/vorschrift/18349-Saechsisches-Informationssicherheitsgesetz, zuletzt abgerufen am 2. August 2019.

Begriffserklärung: Informationssicherheitsbeauftragte/r (ISB)

Die mit der Informationssicherheit beauftragte Person ist für den angemessenen Schutz der IT-Systeme und das Erreichen des angestrebten Informationssicherheitsniveaus verantwortlich.

Die Analyse vorhandener Informationssicherheitsmaßnahmen und deren gegebenenfalls notwendige Optimierung stehen im Zentrum der Arbeit. Dabei werden die sicherheitsrelevanten Komponenten sowie relevante Bedrohungen und Risiken definiert und entsprechende Sicherheitsziele und Verfahrensbeschreibungen formuliert und implementiert. Darüber hinaus ist die zuständige Person auch für die Sensibilisierung von Mitarbeitenden zuständig.

Die/Der Informationssicherheitsbeauftragte fungiert dabei als Bindeglied zwischen der verantwortlichen Person, der IT-Abteilung sowie den Nutzerinnen und Nutzern.

ORP – Organisation und Personal

Gezielte Maßnahmen minimieren zentrale Informationssicherheitsrisiken für Schulen. Diese Maßnahmen können jedoch nur wirksam umgesetzt werden, wenn die notwendigen Rollen und Prozesse innerhalb der Organisation verankert und die notwendigen Ressourcen zur Verfügung gestellt werden. Prinzipiell gilt es, sämtliche Mitarbeitenden einer Organisation zu sensibilisieren und in den konkreten Umgang mit dem Authentisierungsverfahren einzuweisen. Die Benennung einer/eines Informationssicherheitsbeauftragten ist allerdings zentral.

Zentrale Aufgaben

— Rollen und Prozesse klar definieren
— Mitarbeitende sensibilisieren
— Überprüfung der Vertrauenswürdigkeit bei besonderen Vertrauensstellungen

Quick-Check 03 Organisation

Quick-Check 02 Sensibilisierung

Beschreibung der Schicht „Rollen und Berechtigungen“

Die Klärung von Rollen und Rechten ist essentiell für die Implementierung eines ISMS. Hier wird festgeschrieben, wer mit welchen Befugnissen für die Implementierung, das Monitoring und die Anpassung von sicherheitsrelevanten Prozessen verantwortlich ist.

Innerhalb des Schulbetriebes sollte vor allem die Leitungs- / Management-Position als für ISMS hauptverantwortlich besetzt sein. Diese Position kann entweder bei der Schulleitung und/oder bei der Schulverwaltungsleitung angesiedelt sein.

und trägt Sorge für die Bereitstellung der personellen und finanziellen Mittel und Ressourcen. Die Leitung sollte stets umfangreich informiert werden, denn ihr obliegt die Verantwortung für die strategische Ausrichtung der Organisation.

Neben dieser Rolle sollten auch die Verantwortlichkeiten jedes Mitarbeitenden innerhalb der Sicherungsprozesse festgelegt werden, zum Beispiel für die Fragen:

— Wie verhalte ich mich, wenn mein Gerät durch Schadsoftware infiziert wurde?
— Welche Standards für Passwörter liegen vor?
— An wen wende ich mich, wenn ich Sicherheits-Updates benötige?

Je klarer diese Prozesse sind, umso besser kann die ständige Prüfung erfolgen.

Mitarbeitende und verantwortliche Personen sind regelmäßig zu schulen, wobei dies für die zuständigen Administratorinnen und Administratoren mit größerer Intensität erfolgen sollte. Gleichzeitig muss regelmäßig geprüft werden, ob die Schulungsangebote auf dem aktuellen Stand und vollständig sind.

Hinzu kommt die Notwendigkeit festzulegen, wie die Dokumentation innerhalb der zuständigen Abteilung erfolgen soll und wie die Leitung zu informieren ist.

Beschreibung der Schicht „Rollen und Berechtigungen“

Besondere Hinweise laut Profil „Basis-Absicherung Kommunalverwaltung“:

ORP.1	ORP.2	ORP.3	ORP.4	ORP.5
Organisation **A1 – A4, A15**	Personal **A1 – A5, A14, A15**	Sensibilisierung und Schulung **A1, A3, A6**	Identitäts- und Berechtigungsmanagement **A1 – A9, A19, A22, A23**	Compliance Management (Anforderungsmanagement) **A1 , A2**

CON – Konzepte und Vorgehen

Für Schulträger ist es zentral, einen besonderen Fokus auf die Sicherung von Daten und Datenträgern sowie auf die Absicherung gegen Datendiebstahl, -Missbrauch und -Verlust zu legen. Dabei sind auch das Thema Datenschutz und die Sensibilisierung von Mitarbeitenden, Lehrkräften, Schülerinnen und Schülern für den Umgang mit vertraulichen Daten relevant.

Zentrale Aufgaben

- Nutzende für den Umgang mit vertraulichen Daten sensibilisieren
- Sichere Aufbewahrung von Datenträgern, geeignete Lagermöglichkeiten
- IT-Sicherheit immer mitdenken

Quick-Check 04 Konzepte

Dies gilt nicht nur für digitale Datenträger. Bei einem im Bus vergessenen Klausurenheft handelt es sich auf den ersten Blick vielleicht nicht um einen schweren Verstoß gegen bestehende Sicherheitsvorschriften. Dem Einzelnen könnte die Herausgabe sensibler Informationen – sei sie absichtlich geschehen oder unabsichtlich – erheblich schaden.

Beschreibung der Schicht „Konzepte und Vorgehen“

Der sichere Umgang mit Daten und Informationen ist zentral für das Informationssicherheitsmanagement. Daher gilt es, feste Regeln für die sorgfältige Dokumentation, die Datensicherung und die Aufbewahrung von Datenträgern zu etablieren. Hierbei ist ebenfalls die Sensibilisierung der Mitarbeitenden entscheidend. Außerdem sollten Schulträger Prozesse für das Einsammeln nicht mehr gebrauchte Datenträger und für die sichere Archivierung sowie die eventuelle Vernichtung digitale und analoge Daten konzipieren.

Darüber hinaus muss beim Einkauf und bei der Konfiguration von Software-Anwendungen ebenfalls das Thema Informationssicherheit bedacht werden. Auch der interne und externe Informations- und Kommunikationsfluss zwischen Personen muss abgesichert werden. Bei Web-Anwendungen ist ebenfalls auf einen ausreichenden Zugriffsschutz, zum Beispiel durch passende Authentifizierungsmaßnahmen, zu achten.

Im Hinblick auf den Datenschutz besteht die Herausforderung in der Einhaltung der gesetzlichen Vorgaben des Bundesdatenschutzgesetzes (BDSG) und der Datenschutzgrundverordnung (DSGVO).

Der Einsatz von Kryptografie (der Verschlüsselung von Informationen) ist nur bei einem erhöhten Schutzbedarf der betreffenden Daten wichtig.

Besondere Hinweise laut Profil „Basis-Absicherung Kommunalverwaltung“

CON.3	CON.6	CON.9
Datensicherungskonzept **A1 – A5, A12, A14, A15**	Löschen und Vernichten **A1, A2, A11, A12, A13**	Informationsaustausch **A1 – A3**

Dabei ist für die (physische) Aufbewahrung von Daten auf kommunaler Ebene immer auch die Gefahrenlage am Standort zu ermitteln, um geeignete Lagermöglichkeiten auszuwählen. In einer hochwassergefährdeten Schule müsste daher zum Beispiel ein höher gelegener Raum genutzt werden.

Beschreibung der Schicht „Konzepte und Vorgehen“

Darüber hinaus sind laut dem Profil „Basis-Absicherung Kommunalverwaltung“ Regeln für die Festlegung zulässiger Kommunikationspartner zu bestimmen.

Werden Wechseldatenträger verwendet, müssen des Weiteren die Anforderungen aus „SYS 4.5“ angewendet werden.

OPS – Betrieb

Ausreichende Ressourcen sind eine Grundlage des Betriebs einer sicheren Schul-IT. Um alle Informationen stets an alle Veränderungen anpassen zu können, bedarf es eines Kommunikationssystems, über das Informationen zu Sicherheitsvorfällen sowie zu Änderungen an den Systemen schnell und zielgerichtet verteilt werden können. Dies betrifft die Hardware ebenso wie die Software – im Kontext Schule auch die von der Schule selbst beschaffte Software.

Zentrale Aufgaben

- Richtlinie zum Betrieb erstellen
- Schulung aller Admins zu ihrer besonderen Rolle und Verantwortung
- Einheitliche Dokumentationsstruktur erstellen

Quick-Check 05 Betrieb

Für Schulträger ist es darüber hinaus wichtig, eine Richtlinie für alle Systeme, die im Zuständigkeitsbereich des Schulträgers betrieben werden, zu erstellen. Die Informationen zu den lokal an den Schulen betriebenen Servern müssen in diesen Prozess zwingend einbezogen werden ebenso wie die an den Schulen zuständigen IT-Beauftragten. Alle Administratorinnen und Administratoren sollten eine Schulung zum Umgang mit dieser Richtlinie erhalten.

Beschreibung der Schicht „Betrieb“

Die Prüfung der Anforderungen für die Administration, den Betrieb und die Dokumentation ist eine wichtige Voraussetzung für die Informationssicherheit.

Darüber hinaus wird die Kommunikation zum Änderungsmanagement zwischen den Verantwortlichen als zentraler Punkt dargestellt. Gleichzeitig bedarf es der Etablierung von Prozessen, um sicherheitsrelevante Ereignisse rechtzeitig erkennen sowie schnell und vollständig nachvollziehen zu können. Grundlegend ist hier die Formulierung einer Richtlinie zur Erkennung von sicherheitsrelevanten Vorfällen und für die entsprechenden Meldewege.

Eine ordnungsgemäße Durchführung der Administration soll die Leistungsfähigkeit und die Funktionsfähigkeit für den IT-Betrieb sicherstellen. Dies bedeutet, dass Sicherheitsmaßnahmen, wie die Regelung der Zugänge zu schützenswerten Bereichen der IT, konsequent durchgeführt werden müssen. Zudem muss eine klare Regelung für die Vergabe von Administrationsrechten sowie für die Vertretungsregelungen bestehen und nachvollziehbar dokumentiert sein.

Ferner ist es notwendig, die Administratorinnen und Administratoren so zu schulen, dass sie kompetent und mit der entsprechenden Achtsamkeit bezüglich der Sicherheitsthematik in ihrer Rolle umgehen. Jede neu eingeführte Software sollte zunächst getestet und, wenn für sicher befunden, von der IT-Administration freigegeben werden.

Zur Sicherung der Schutzmaßnahmen und bei allen Änderungen des Aufbaus der IT ist eine ordnungsgemäße und vollständige Dokumentation für die Nachvollziehbarkeit der Handlungen unerlässlich. Die Archivierungsdauer (oft mehrere Jahre) ist für viele Verwaltungsbereiche vom Gesetzgeber vorgeschrieben. Es gilt, darauf zu achten, dass die Sicherung von Daten auf langlebigen Speichermedien erfolgt.

Besondere Hinweise laut Profil „Basis-Absicherung Kommunalverwaltung“

OPS.1.1.2	**OPS.1.1.3**	**OPS.1.1.4**	**OPS.1.1.5**
IT-Administration	Patch- und Änderungsmanagement	Schutz vor Schadprogrammen	Protokollierung
A2, A4 – A6, A12, A21, A22	**A1 – A3, A15**	**A1 – A3, A5 – A7**	**A1, A3 – A5, A10**

Beschreibung der Schicht „Betrieb“

OPS.1.2.4	OPS.1.2.5	OPS.2.1	OPS.2.2
Telearbeit **A1, A2, A5**	Fernwartung **A1 – A3, A5, A7 – A9, A19**	Outsourcing für Kunden **A1 – A4, A6 – A10, A12, A15**	Cloud-Nutzung **A1 – A4, A6, A8, A9, A13, A14**

Für die kommunale IT ist es zentral, dass genügend Ressourcen für den IT-Betrieb bereitgestellt werden.

Darüber hinaus ist es notwendig, eine einheitliche Dokumentationsstruktur und ein einheitliches Regelwerk für die Wartungsarbeit und die Fernwartungsvorgänge zu erstellen. Die Dokumentation sollte zentral und geschützt archiviert werden und auch alle Wartungsarbeiten sowie die Beaufsichtigungspflicht des Wartungspersonals beinhalten. Das Gleiche gilt für die Fernwartung der Geräte. Die Aufgaben von Anwendungs- und Systemadministratorinnen und -administratoren müssen zwingend aufgeteilt werden.

Es ist außerdem elementar, dass die Nutzerinnen und Nutzer (im Fall der Schul-IT Lehrkräfte, Schülerinnen und Schüler oder Verwaltungsmitarbeitende) die Antivirenprogramme nicht selbstständig verändern können und wissen, wem sie einen möglichen Sicherheitsvorfall melden können.

Vielerorts können Mitarbeitende heutzutage die ihnen zur Verfügung gestellten mobilen Endgeräte mit nach Hause nehmen. Hier sollte die „Empfehlung zum sicheren mobilen Arbeiten im Homeoffice“ des BSI beachtet werden.

Werden für betriebliche Aufgaben externe Dienstleister eingesetzt, muss im Vertrag auch die Beachtung der IT-Sicherheit geregelt sein. Viele Schulträger nutzen Cloud-Dienste für die Umsetzung der pädagogischen Anforderungen in Schulen. In diesem Zusammenhang müssen der Art und dem Ort der Verarbeitung der Daten besondere Aufmerksamkeit geschenkt werden.

DER – Detektion und Reaktion

Für Schulträger ist es wichtig, sich rechtzeitig Strategien zur Erkennung und Behebung von informationssicherheitsrelevanten Vorfällen zu erarbeiten. Großangelegte Angriffe auf Schulträger erscheinen heute vielleicht unwahrscheinlich. Kleine Verstöße oder Fehlverhalten führen teilweise aber bereits zu Sicherheitslücken, aufgrund derer sich Angreifende Zugang zum System verschaffen können. In dieser Hinsicht empfiehlt es sich, darüber nachzudenken, Verwaltungsnetze, die oft mit anderen Verwaltungsbereichen einer Kommune kommunizieren können oder verbunden sind, vom pädagogischen Netzwerk zu trennen.

Zentrale Aufgaben

- Strategie zur Erkennung und Beseitigung von Störfällen aufstellen
- Überblick über die gesamte Systemlandschaft des Schulträgers erstellen
- Trennung der Schulverwaltungsnetze von den pädagogischen Netzen

Quick-Check 10 Detektion und Reaktion

Empfehlenswert für die Schulträger ist die Einrichtung eines geschulten Leitungsgremiums, das einen Überblick über die komplette IT-Landschaft des Schulträgers und der trägereigenen Schulen hat. Vor allem bei Vorfällen im Hinblick auf Nutzerkonten und Zugangswege ist es wichtig, dass ein Zugang zu den Systemen in jedem Fall besteht, um im Ernstfall eingreifen und Passwörter sperren zu können.

Da in den meisten Fällen beim Schulträger kein eigenes IT-Forensik-Team vorhanden ist, gilt es für den Fall eines schwerwiegenden Angriffs, Verträge mit externen Dienstleistern abzuschließen. Wenn bereits Dienstleister mit Support- und Service-Aufgaben betraut sind, gilt es zu prüfen, welche Möglichkeiten dort zur Umsetzung der Bausteine bestehen oder bereits etabliert sind.

Beschreibung der Schicht „Detektion und Reaktion“

Für die Aufrechterhaltung der Informationssicherheit ist es wichtig, sicherheitsrelevante Ereignisse zu erkennen und darauf zu reagieren. Ein sicherheitsrelevantes Ereignis ist eines, das sich auf die Informationssicherheit auswirkt und die Vertraulichkeit, Integrität oder Verfügbarkeit der Daten beeinträchtigen kann. Typische Folgen sind ausgespähte, manipulierte oder zerstörte Informationen.

Ein solches Ereignis entsteht zum Beispiel durch eine Fehlkonfiguration, durch die vertrauliche Informationen offengelegt oder kriminelle Handlungen möglich werden. Die Ursachen für diese Ereignisse sind vielfältig. Dazu zählen zum Beispiel der Angriff mit Schadsoftware von außen, veraltete IT-System-Infrastrukturen oder Angriffe innerhalb eines Netzwerks.

Auch Sicherheitslücken (Zero-Day-Angriffe) in Programmen, können ausgenutzt werden. Eine ernstzunehmende Gefährdung sind auch Advanced Persistent Threats (APT). Dies sind zielgerichtete Cyber-Angriffe, bei denen sich die Angreifenden dauerhaften Zugriff verschaffen und diesen sukzessive ausweiten. Solche Angriffe zeichnen sich durch einen hohen Ressourceneinsatz und erhebliche technische Fähigkeiten der Angreifenden aus und sind oft nur unter Zuhilfenahme von Spezialfirmen zu detektieren und zu beheben.

Aber auch das Fehlverhalten von Benutzerinnen und Benutzern sowie von Administratorinnen und Administratoren oder externen Dienstleistern kann Systemparameter sicherheitskritisch verändern. Ebenso sind die Vernachlässigung und die unzureichende Absicherung von schutzbedürftigen Räumen und Gebäuden durchaus gefährlich.

Um diese Vorfälle zu verhindern, bieten die Bausteine dieser Schicht Schritte und Prozesse an, die umgesetzt werden können, um die eigenen Systeme laufend zu überwachen, um Schwachstellen und Vorfälle schon frühzeitig zu erkennen, zu melden und schließlich auch zu beheben. Dabei kommen oft spezielle Software-Lösungen zum Einsatz.

Neben der Software müssen auch Hardware und Gebäude überwacht werden. Gerade bei größeren Sicherheitsvorfällen oder sicherheitsrelevanten Ereignissen müssen oft externe Dienstleister einbezogen werden, um forensische Schritte einzuleiten oder ressourcenreiche und komplexe Angriffe von außen zu stoppen.

Besondere Hinweise laut Profil „Basis-Absicherung Kommunalverwaltung“

DER.2.1
Behandlung von Sicherheitsvorfällen
A1 – A6

Es sind keine weiteren Besonderheiten benannt.

3.2.2 Die Schichten der Systembausteine im BSI

APP – Anwendungen

Für Schulträger ist es wichtig, den Einsatz von Software-Komponenten genau zu planen und alle beteiligten IT-Fachleute, Datenschützerinnen und -schützer, IT-Verantwortlichen, Nutzerinnen und Nutzer in die Planung einzubeziehen. Dies bedeutet, dass ein Schulträger über jegliche Software, die in den Schulen vorhanden ist, Kenntnis haben muss.

Zentrale Aufgaben

— Nur auf Sicherheit geprüfte und notwendige Software in das System einbinden
— Zwei-Browser-Strategie einsetzten
— Besonders auf Sicherheit bei Office-Pro-

Quick-Check 08 Anwendungen

Da Schulen teilweise auch selbständig Software beschaffen können oder kostenlose Software nutzen, ist es sinnvoll einen Meldevorgang für Schulen festzulegen. Ferner sollte eine genaue Liste der Zugriffberechtigungen angefertigt werden, die tagesaktuell an Änderungen angepasst werden kann.

Werden bezüglich des Software-Einsatzes neue Anforderungen an den Schulträger herangetragen, müssen diese dokumentiert und mit dem bestehenden System abgeglichen werden. Vor dem Erwerb von Software sollte immer eine Sicherheitsüberprüfung durchgeführt werden.

Einen besonderen Stellenwert im Schulalltag haben vor allem Microsoft Office-Produkte, die in unterschiedlicher Form in fast allen Schulen und Schulverwaltungen eingesetzt werden. Hier sollten bei der Ausschreibung und der Beschaffung die Interaktion mit dem bestehenden und die Integration in das bestehende System im Anforderungskatalog aufgezeigt werden. Zudem muss darauf verwiesen werden, dass alle Sicherheitsmechanismen greifen müssen.

Beschreibung der Schicht „Anwendungen“

„Anwendungen“ ist ein Oberbegriff für Software, die Funktionen für Nutzerinnen und Nutzer oder andere Anwendungen/Applikationen ausführt. Dazu gehören auch Angebote wie Apps auf mobilen Endgeräten, Web-Anwendungen und Web-Services. Anwendungen können proprietäre Programme (z. B. Microsoft-Office) oder Open-Source-Produkte (z. B. LibreOffice) sein.

Unter dem Sicherheitsaspekt sollte grundsätzlich nur Software in das System integriert werden, die notwendig ist, da jede Software potenziellen Angreifenden Möglichkeiten bietet, Schadsoftware zu implementieren. Diese kann zum Beispiel Daten verändern oder „absaugen“, die Kommunikation abhören oder das gesamte System unbrauchbar machen. Das bedeutet, dass nicht nur die Software insgesamt auf ihre Notwendigkeit hin geprüft werden sollte, sondern auch einzelne Komponenten der Software, wie zum Beispiel Programmerweiterungen, genauer kontrolliert werden sollten.

Darüber hinaus ist es wichtig, die Möglichkeiten der Speicherung der Daten auf sichere Datenspeicher zu begrenzen. Dies gilt für jegliche Software, die im pädagogischen und im administrativen Bereich eingesetzt wird. Sollte Software selbst programmiert werden, empfiehlt es sich, in die Planung die Erstellung eines Sicherheitskonzepts einzubeziehen.

Zum reibungslosen Betrieb der Software werden außerdem vielfach weitere Dienste benötigt, die die Nutzung der Anwendungs-Software auf dem System ermöglichen. Das sind Dienste beziehungsweise Komponenten wie das Active Directory, OpenLDAP, Web- und Fileserver sowie Kubernetis. Da diese Komponenten übergreifend Daten von Nutzerinnen und Nutzern verwalten, ist es hier besonders wichtig, den Aufbau und die Integration der Dienste genau zu planen – unter Einbeziehung von IT-Administratorinnen und -administratoren sowie Datenschützerinnen und -schützern.

Es empfiehlt sich außerdem, ein gut dokumentiertes Berechtigungskonzept zu erarbeiten, um einen Überblick über die Systemzugriffe zu erhalten. Für die IT-Administration sind besonders sichere Passwörter erforderlich, um einen hohen Schutz zu gewährleisten. Während des Betriebs ist eine gute Dokumentation jeglicher Änderungen und aller Sicherheitsvorfälle dringend notwendig.

Auch E-Mail-Server sind potenzielle Angriffspunkte. Sie übernehmen das Senden und Empfangen von E-Mails mithilfe sogenannter Protokolle wie zum Beispiel dem Post Office Protocol (POP) und dem Simple Mail Transfer Protocol (SMTP). Durch unzureichende Planung, fehlerhafte Einstellungen oder gestörte Übertragungswege kann Schadsoftware über E-Mails in das System gelangen. Diese kann dazu führen, dass E-Mails von Unbefugten mitgelesen oder manipuliert werden.

Darüber hinaus kann sich Schadsoftware in den Anhängen von Mails verstecken. Aus diesem Grund sind eine sichere Konfiguration, der sichere Betrieb, ein Spam- und ein Virenschutz sowie die Sicherung und die Archivierung von Daten eine Notwendigkeit, um das System und damit die Daten der Nutzerinnen und Nutzer zu schützen.

Besondere Hinweise laut Profil „Basis-Absicherung Kommunalverwaltung“

APP.1.1 Office-Produkte **A2, A3, A12, A13, A17**	**DER.1.2** Web-Browser **A1 – A3, A6, A12, A13**	**APP.2.1** Allgemeiner Verzeichnisdienst **A1 – A6**	**APP.3.3** Fileserver **A2, A3, A8, A15**
APP.5.3 Allgemeiner E-Mail-Client und -Server **A1 – A5**	**APP.6** Allgemeine Software **A1 – A6**		

Beschreibung der Schicht „Anwendungen“

Dabei sind einige zusätzliche Punkte zentral: Zum einen erhalten Behörden täglich eine Vielzahl von Nachrichten, teils aus unsicheren Quellen. Zum anderen werden gerade im Schulalltag viele Dokumente über die Netze des Schulträgers / der Schulen ausgetauscht. Da es nicht möglich ist, Dokumente aus externen Quellen in Echtzeit zu prüfen, ist es notwendig, alle Nutzerinnen und Nutzer (Verwaltungsmitarbeitende, Lehrkräfte, Schülerinnen, Schüler und Eltern) für das Thema IT-Sicherheit zu sensibilisieren und darin zu schulen.

Ähnlich verhält es sich mit Online-Quellen. Beim Öffnen und Weiterleiten ist besondere Vorsicht geboten. Nachrichten und Anhänge sollten nur in einem geschützten Modus geöffnet werden. Bei der Weiterleitung von E-Mails muss der Datenschutz berücksichtigt werden.

In fast allen Schulen werden darüber hinaus heutzutage Web-Browser eingesetzt, um zum Beispiel im Internet zu recherchieren. Diese können über Schwachstellen verfügen und angegriffen werden. Um schnell auf solche Angriffe reagieren zu können, sollte eine Zwei-Browser-Strategie eingesetzt werden, sodass ein Browser im Notfall abgeschaltet werden kann, ohne dass der Schulbetrieb unterbrochen werden muss. Eventuell in Office-Produkten integrierte Cloud-Speicher-Funktionen sollten grundsätzlich deaktiviert werden.

Besonderes Augenmerk sollte der Schulträger auch auf die folgenden Bestandteile der IT legen: auf den allgemeinen Verzeichnisdienst, die Fileserver, auf WLAN (lokales, kabelloses Netzwerk) und auf VPN (virtuelles privates Netzwerk). Hier gilt es, zeitnah die Anhebung des Sicherheitsniveaus über die Basis-Absicherung mindestens auf ein Standard-Absicherungsniveau zu planen – und zu prüfen, ob die genannten IT-Bestandteile auf dem neuesten Stand der Sicherheitstechnik sind oder ob Sicherheitslücken bestehen.

SYS – IT-Systeme

Schulträger müssen das gesamte IT-System unter Berücksichtigung eines Sicherheitskonzepts planen und alle Änderungen und Störungen protokollieren, um Angriffe abwehren beziehungsweise verhindern zu können. Für die Informationssicherheit ist es wichtig, dass alle Systeme und Komponenten sicher konfiguriert sind und einem Änderungsmanagement unterliegen.

Zentrale Aufgaben

- Gute Planung des gesamten IT-Systems unter Berücksichtigung des IT-Sicherheitskonzepts
- Notfallplan einsetzen
- Frei zugängliche Komponenten durch Authentifizierung schützen

Quick-Check 07 IT-Systeme

Es ist darüber hinaus wichtig, einen Notfallplan zu erstellen und einen/eine Notfallnutzer/in zu benennen. Bei einem Sicherheitsvorfall ist die Reaktionsgeschwindigkeit ein sehr wichtiger Faktor, da über mobile und stationäre Endgeräte häufig auf das gesamte IT-System zugegriffen werden kann. Auch Drucker, als Teil der Hardware, sind potenzielle Angriffspunkte und durch ihre Platzierung, etwa in offenen Computerräumen, meist schwierig zu schützen. Eine verpflichtende Authentifizierung vor dem Druckvorgang könnte Abhilfe schaffen.

Um Datenverlusten vorzubeugen, sollten alle Speicherlösungen und damit auch die Wechseldatenträger einem Sicherheitskonzept unterliegen und sicher gelagert werden. Jeder Server sollte über eine unterbrechungsfreie Stromversorgung (USV) verfügen, sodass kurzfristige Stromausfälle abgefangen werden können. Hier ist es wichtig, auch die Server, die den Schulen zur Verfügung gestellt werden, mit zu berücksichtigen.

Wenn IT-Komponenten außer Betrieb genommen werden müssen, sollten zuvor sensible Daten gelöscht werden, sodass Angreifende diese nicht auslesen können. Laut Profil „Basis-Absicherung Kommunalverwaltung“ erhöht der Einsatz einer USVs die Verfügbarkeit der Daten drastisch.

Beschreibung der Schicht „IT-Systeme“

Die Bausteine dieser Schicht beschreiben Sicherheitsmaßnahmen für IT-Systeme und deren Komponenten, wobei die Art des Betriebssystems bezüglich dieser keine Rolle spielt.

Die für die Systeme notwendigen Server müssen in abgeschlossenen Räumen stehen, zu denen nur Berechtigte Zutritt haben, und sie dürfen nie als Arbeitsplatzrechner genutzt werden. Dies gilt auch für die Aufstellung von Speichersystemen.

Bei der Bereitstellung von Betriebskomponenten ist darauf zu achten, dass es sich bei diesen ausschließlich um für den Betrieb der IT-Systeme zwingend erforderliche Produkte handelt.

Das gesamte Netz sollte permanent überwacht werden, sodass ein schnelles gezieltes Eingreifen bei Angriffen möglich ist. Unabhängig vom Betriebssystem muss ein eindeutiges Authentifizierungsverfahren implementiert werden. Gleichzeitig sollten Zugriffsrechte soweit wie möglich eingeschränkt werden, um Angriffe einzuschränken.

Auch die mobilen Endgeräte müssen unter Berücksichtigung eines Sicherheitskonzepts betrieben werden. So sind Authentifizierungs- und Identifikationsmechanismen genauso notwendig wie die Absicherung der Startprozesse gegen Manipulation. Auch hier ist das Angebot der Funktionen auf das Nötigste zu reduzieren. Laptops, die außerhalb der Organisation eingesetzt werden, müssen über eine Firewall verfügen, deren Warnmeldungen für die Nutzerinnen und Nutzer verständlich sind. Bei Druckern, Kopierern und Multifunktionsgeräten ist deren Standort so zu wählen, dass unberechtigte Personen keinen Zugriff auf die Geräte haben.

Bei der Beschaffung jeglicher Art von mobilen Endgeräten sollte darauf geachtet werden, ob und wie lange der Hersteller Sicherheits-Updates zur Verfügung stellt.

Wenn mobile Endgeräte über ein Mobile-Device-Management-System (MDM) betrieben werden, muss auch das unter Berücksichtigung der Sicherheitsanforderungen geplant werden. Ferner sollte eine Strategie vorliegen, die genau beschreibt, wie welche mobilen Endgeräte in das MDM eingebunden und unterstützt werden.

Bei integrierten Cloud-Lösungen ist es besonders wichtig, die für den Betrieb geeignete Version zu nutzen und ein Datensicherungskonzept zu erstellen.

Bei eingebetteten Systemen, wie zum Beispiel Chipkarten, sind vor allem die Zuständigkeit und die Verhaltensregeln für die Nutzerinnen und Nutzer zu klären.

Wechseldatenträger wie CD-ROMs, DVDs, Speicherkarten, Magnetbänder oder USB-Sticks müssen sicher aufbewahrt werden. Die darauf enthaltenen Daten sollten protokolliert und die Mitarbeitenden darüber informiert sein, welche Daten auf welchen Datenträgern vorhanden sind. Für den Fall des Verlusts eines dieser Datenträger müssen die Meldewege vorher klar definiert sein. Alle gespeicherten Daten müssen angemessen verschlüsselt werden.

Besondere Hinweise laut Profil „Basis-Absicherung Kommunalverwaltung“

SYS.1.1 Allgemeiner Server **A1, A2, A5, A6, A9, A10, A15, A21, A25**	**SYS.2.1** Allgemeiner Client **A1, A3, A6, A8, A14, A24, A27, A28, A42**	**SYS.1.5** Virtualisierung **A2 – A5, A12**	
SYS.3.1 Laptops **A1, A3, A6, A8 – A10, A12, A13**	**SYS.3.2.1** Allgemeine Smartphones und Tablets **A1 – A8**	**SYS.3.3** Mobiltelefon **A1 – A4**	**SYS.4.1** Drucker **A1, A2, A4, A7, A11, A14, A18, A22**

Da in der kommunalen IT und damit auch in der Schul-IT eine Vielzahl von sensiblen Daten verarbeitet werden, sind zudem laut dem Profil „Basis-Absicherung Kommunalverwaltung“ weitere Besonderheiten zu bedenken: Zum einen ist der Zugriff auf die Systeme, Geräte und die Netzwerke zu steuern. Zugriffsrechte müssen auf den relevanten Personenkreis beschränkt und Passwörter eingerichtet werden. Dies gilt auch für den – vor allem externen – Zugriff auf Geräte wie Drucker oder auf Daten. Bei der Aufstellung von Geräten in öffentlichen Räumen ist besondere Vorsicht geboten.

Die Zugriffsrechte für Administratorinnen und Administratoren sollten besonders zielgerichtet vergeben werden. Ändern sie etwas an einem System, kann das weitaus mehr Schaden verursachen, als bei anderen Personen. Sollten sie Geräte per Fernzugriff warten und konfigurieren, ist eine Authentisierung zwingend erforderlich.

Änderungen müssen autorisiert und dokumentiert werden. Nur so ist eine Fehlerbehebung im Nachhinein möglich. Das Einführen von automatischen Updates ist vorher durch die Administratorinnen und Administratoren zu genehmigen.

Beschreibung der Schicht „IT-Systeme“

Werden Server, Clients (Programm) oder Datenträger entsorgt oder aus dem Verkehr genommen, ist darauf zu achten, dass die darauf befindlichen Daten nicht wiederhergestellt werden können. Bei Entsorgung von Geräten wie Druckern ist zudem Baustein „CON.6.A2“ zu berücksichtigen.

Gleichzeitig müssen Daten von mobilen Endgeräten wie Laptops regelmäßig mit den Datenbanken der Verwaltung synchronisiert werden.

Da einzelne infizierte Rechner ein ganzes IT-Netzwerk befallen können, ist es notwendig, die Nutzung von fremden Datennetzen auf mobilen Verwaltungsgeräten einzuschränken und klar zu definieren.

NET – Netze und Kommunikation

Für Schulträger ist die Planung oft ein schwieriges Unterfangen, da in vielen Fällen Teile des Netzwerks schon bestehen und nicht immer gut dokumentiert sind.

Um den Überblick zu behalten, ist es notwendig, vorhandene Strukturen in neu zu erstellende Netzpläne aufzunehmen und so ein umfassendes Bild zu zeichnen. Jegliche Änderungen sollten durch eine verantwortliche Person dokumentiert werden, sodass keine Schwachstellen entstehen oder vorhandene übersehen werden können.

Zentrale Aufgaben

- Sorgfältige Planung und Sicherung der Netze
- Netzwerkmanagement
- Einführung von Richtlinien für Passwörter und Accounts

Quick-Check 09 Netze & Kommunikation

Da über die Netzwerke der Schulträger auf der einen Seite vertrauliche Daten gesendet werden und sie auf der anderen Seite von vielen unterschiedlichen Nutzendengruppen (Verwaltungsmitarbeitende, Lehrkräfte, Schülerinnen, Schüler sowie evtl. Eltern) genutzt werden, ist es absolut notwendig, Sicherheitsrichtlinien aufzustellen und diese regelmäßig zu prüfen.

Darüber hinaus sollte ein klarer Notfallplan erstellt werden, um bei erfolgreichen Angriffen schnell und zielgerichtet reagieren zu können.

Beschreibung der Schicht „Netze und Kommunikation“

Die Netzarchitektur und das Netzdesign erfordern eine sehr sorgfältige Planung. Diese beinhaltet die Struktur, den Aufbau und alle zu integrierenden Komponenten. Festgehalten wird diese Planung in Netzplänen, Beschreibungen des Aufbaus sowie Richtlinien zum Betrieb und zu Sicherheitsvorschriften.

Vor der Erstellung des Plans sollten alle Anforderungen an das Netzwerk und an die zugehörigen Komponenten erfasst und dokumentiert werden, um eine solide Grundlage für eine bedarfsgerechte Planung zu schaffen.

Darüber hinaus sollte festgelegt werden, welche Bereiche physisch oder auch logisch voneinander getrennt sein müssen, um eine hohe Sicherheit der Netzstruktur zu gewährleisten. Auch die Auswahl der Standorte der einzelnen Netzwerk-Komponenten wie Server, Switches, Router und Accesspoints ist nicht trivial: Zum einen müssen sie gut erreichbar sein und eine ausreichende Versorgung aller Endgeräte sichern und zum anderen müssen sie vor dem Zugriff Unbefugter geschützt sein.

Für alle in dieser Schicht dargestellten Bereiche ist es daher notwendig, Sicherheitsrichtlinien zu schaffen.

Darüber hinaus sollten alle messbaren Aktivitäten gut protokolliert und die Grundkonfiguration sowie jegliche Änderungen dieser nachvollziehbar dokumentiert werden. Alle Möglichkeiten des Zugriffs auf Komponenten des Netzwerks müssen über eine zeitgemäße Verschlüsselung durch ein kryptografisches Verfahren verfügen; alle Zugriffe müssen erfasst werden.

Ferner sollten Administrationsschnittstellen logisch von anderen Schnittstellen getrennt werden. Eine übergreifende Sicherheitsrichtlinie, die das gesamte Netzwerk und alle Zugriffsmöglichkeiten sowie Gefährdungen beschreibt, sollte hinterlegt werden.

Beschreibung der Schicht „Netze und Kommunikation“

Besondere Hinweise laut Profil „Basis-Absicherung Kommunalverwaltung“:

NET.1.2 Netzmanagement **A1, A2, A6 – A10, A18**	**NET.2.1** WLAN-Betrieb **A13**	**NET.3.1** Router und Switches **A1, A4 – A9**	**NET.3.2** Firewall **A1 – A4, A6 – A10, A14, A15, A17, A18, A20, A22,**
NET.3.3 VPN **A1 – A5, A7, A11**	**NET.4.1** TK-Anlagen **A1, A2, A7, A8, A10, A12, A15 – A18**	**NET.4.2** VoIP **A1, A3 – A5, A8, A11, A13, A16**	**NET.4.3** Faxgeräte und Faxserver **A1 – A3, A8**

Für die Umsetzung der Anforderungen aus den Bausteinen dieser Schicht in der kommunalen IT identifiziert das Profil einige Besonderheiten. Der Einsatz von VPN-Lösungen ist frühzeitig und sorgfältig zu planen, damit Probleme nicht erst beim Einsatz selbst auftreten und bis zur Behebung durch Angreifende ausgenutzt werden können. Zudem ist bei der Nutzung eines VPN auf eine solide Vertragsbasis zu achten, damit zugesicherte Leistungen eingehalten werden.

Externe Netzwerke müssen sicher verschlüsselt angebunden werden, damit Unbefugte keinen Zugriff erhalten. Bei der Einrichtung einer Firewall ist darauf zu achten, dass die Protokolle aktuell sind und alte Protokolle gelöscht werden, um keine Lücken zu schaffen. Alle Anforderungen an die Firewall sowie die Verantwortlichkeit für die Firewall sind zu dokumentieren.

Es muss fortlaufend überwacht werden, ob und wo sich neue Sicherheitslücken auftun, um diese gegebenenfalls durch die geeigneten Patches (digitale „Korrekturwerkzeuge“) schließen zu können. Passwörter sind in regelmäßigen Abständen zu aktualisieren, die Nutzerinnen und Nutzer auf den Ablauf von deren Gültigkeit hinzuweisen und für den sicheren Umgang mit den Netzen zu sensibilisieren.

INF – Infrastruktur

Zentrale Aufgaben

— Mobile Arbeitsplätze erfordern Strukturen für Verlustmeldungen und korrekte Entsorgung
— Abschließbare Räumlichkeiten für sicherheitsrelevante Komponenten
— Brandschutzkonzept für Serverraum / Klimatisierung

Quick-Check 06 Gebäude & Arbeitsplatz

Die Digitalisierung des Bildungswesens bedingt ein starkes Anwachsen der digitalen Infrastruktur bei Schulträgern und in Schulen. Unabhängig von einer zunehmenden Zahl von Servern führt die Digitalisierung auch zu einer stärkeren Verkabelung in Schulgebäuden. Diese Strukturen gilt es vor Schaden durch Feuer, Wasser oder Diebstahl zu bewahren. Dabei spielt der Brandschutz eine besondere Rolle und sollte bei Schulneubauten von Anfang an sorgfältig mitgeplant werden. IT-Systeme und vor allem deren Verkabelung sind brandsicher zu gestalten sowie entsprechend zu lüften und zu temperieren. Schülerinnen und Schüler sowie Lehrkräfte sollten darin geschult werden, wie sie sich bei einem Feueralarm und anderen Gefahrenmeldungen verhalten müssen, um etwa im Falle eines Brandes sicher und ruhig zu reagieren.

Gleichzeitig gilt es, die Server und Verkabelungen planvoll und effektiv zu verlegen, um Reparaturen und Ausbauten möglich zu machen. Im Bereich der Verkabelung sehen sich viele Schulen auch vor der Herausforderung der Dimensionierung für die nächsten Jahrzehnte. Neu verlegte Kabeltrassen sind so zu wählen, dass sie den Anforderungen einer stetig wachsenden Schul-IT auch in den kommenden Jahren noch gerecht werden können.

Auch das Thema Diebstahlschutz dürfte allgemein für Schulen wichtiger werden. Gerade die steigende Zahl an wertvollen IT-Komponenten machen Schulen zu einem beliebten Einbruchsziel, zumal es feste Zeiten

wie Schulferien oder Wochenenden gibt, in denen sich in der Regel niemand in den Gebäuden aufhält. Erschwerend kommt hinzu, dass in vielen Schulen der Schulhof auch außerhalb der Schulzeit frei zugänglich ist.

Darüber hinaus ist das Schlüsselmanagement in Schulen mitunter eine Herausforderung, da eine Vielzahl von Personen – etwa Lehrkräfte, weitere pädagogische Kräfte sowie Hausmeisterinnen und Hausmeister – Zugang zum Gebäude haben. Alle diese Personen sollten dafür sensibilisiert werden, immer Türen und Fenster zu verschließen und keine sicherheitsrelevanten Informationen liegenzulassen. Auch das Arbeiten von zu Hause erfordert Sensibilität und die Umsetzung geeigneter Maßnahmen.

Beschreibung der Schicht „Infrastruktur“

Die IT-Infrastruktur, bedarf stets der mindestens Absicherung gegen Ausfall, Störung, Manipulation und Datendiebstahl um Verfügbarkeit, Vertraulichkeit und Integrität zu sichern.

Für Datenträger, sowohl digital, als auch auf Papier, gilt es außerdem den unbefugten Zugriff zu schützen und Verschmutzung und Schäden von den gelagerten Daten fernzuhalten.

Die entsprechenden Räume sind daher gegen Einbruch zu sichern und mit Zutrittskontrollen zu versehen.

Bei den Maßnahmen gegen Diebstahl spielen hier auch die Mitarbeitenden eine entschiedene Rolle, da es gilt, Türen und Fenster beim Verlassen von Räumen zu schließen und Informationen nicht herumliegen zu lassen. Auch beim Arbeiten zu Hause und unterwegs gilt es Sicherheitsmaßnahmen einzuhalten, um die Informationssicherheit nicht zu gefährden.

Eine wichtige Rolle spielt hier aber auch der Schutz vor Elementarschäden, besonders durch Brände. Dabei können IT-Komponenten und Datenträger nicht nur durch direkten Kontakt mit Feuer beschädigt werden, sondern auch durch Rauch oder durch Löscharbeiten in Mitleidenschaft gezogen werden.

Besondere Hinweise laut Profil „Basis-Absicherung Kommunalverwaltung“

INF.1 Allgemeines Gebäude **A1 – A8, A10**	**INF.2** Rechenzentrum sowie Serverraum **A1 – A11, A17, A29**	**INF.5** Raum sowie Schrank technische Infrastruktur **A1 – A7, A9**	**INF.6** Datenträgerarchiv **A1 – A4**	**INF.7** Büroarbeitsplatz **A1, A2, A5 – A7**

INF.8 häuslicher Arbeitsplatz **A1 – A3, A5**	**INF.9** mobiler Arbeitsplatz **A1 – A6**	**INF.10** Besprechungs-, Veranstaltungs- und Schulungsraum **A1, A3, A6, A7**	**INF.11** Allgemeines Fahrzeug **A1 – A4**

für den Bereich kommunale IT ergeben sich einige Besonderheiten. An dieser Stelle seien nur eine ausgewählte Anzahl an Besonderheiten genannt, die so auch für die Schul-IT besondere Relevanz haben. Da in der Kommunalverwaltung und in Schulen stets reger Publikumsverkehr herrscht, ist es wichtig, besonders sensible Komponenten nicht zu exponiert oder in gefährdeten Bereichen unterzubringen.

Auch Datenträger sind unzugänglich aufzubewahren. Der Zugang zu den internen Verwaltungsnetzen darf nur von dafür vorgesehenen Arbeitsplätzen möglich sein. Druckerräume dürfen keine „Einfallstore“ zum internen Verwaltungsnetz bieten. Außer bei Datenarchiven und Schutzschränken, kann allerdings in der Regel darauf verzichtet werden, jeden einzelnen Zutritt zum Raum oder Zugriff auf einen Schrank zu dokumentieren.

Vertrauliche Informationen sind außerdem sicher zu entsorgen und zu transportieren. Dies muss auch beim häuslichen Arbeitsplatz möglich sein. Gehen Unterlagen verloren, ist der Verlust zeitnah zu melden, damit geeignete Maßnahmen eingeleitet werden können.

Mitarbeitende sind zentral im Schutz von sensiblen Daten. Sie müssen darauf achten, dass Bildschirme nicht von Unbefugten eingesehen werden oder das vertrauliche Informationen nicht herumliegen oder zugänglich sind. Sie sind es außerdem, die darauf achten müssen, beim Verlassen von Räumen mit Schutzschränken die Fenster und Türen zu schließen.

Neben den hier dargestellten Schichten gibt es im BSI die Schicht „IND“ (Industrielle IT). Da die Bausteine dieser Schicht die Informationssicherheit von speziellen Maschinen und Software-Lösungen behandelt, die vor allem in der Industrie vorkommen, hat er für die Schul-IT nur eine untergeordnete Rolle. Zwar kann es auch im Schulumfeld vorkommen, dass spezialisierte Maschinen zum Einsatz kommen, zum Beispiel Werksmaschinen im Bereich der beruflichen Ausbildung, allerdings werden diese aufgrund ihres Einsatzes als Schulungswerkzeug eher nicht an ein komplexes Firmennetzwerk angebunden und Schnittstellen zu kritischen Prozessen oder Systemen aufweisen.

Hinweis: Aufgrund der hohen Komplexität und des großen Umfangs an zu verarbeitenden Informationen und zu koordinierenden Umsetzungsmaßnahmen sollten Schulträger und Schulen bei der Einführung eines Informationssicherheitsmanagements über den Einsatz von ISMS-Software-Lösungen nachdenken. Spezialisierte Anbieter stellen Anwendungen bereit, in denen der gesamte Informationsverbund abgebildet werden kann. Außerdem können darin die eingesetzten Hardware-, Software- und Netzwerk-Komponenten jeweils den entsprechenden Bausteinen mitsamt ihren Anforderungen zugewiesen sowie die Umsetzung und alle anfallenden Änderungen dokumentiert werden. Dies erleichtert im Falle einer späteren Auditierung und Zertifizierung (Ansatz 2) auch den Berichtsprozess. Viele Lösungen bieten ebenfalls die Möglichkeit, das Datenschutzmanagement mit darzustellen und zu dokumentieren. Da bei vielen dieser Lösungen eine Vielzahl von Informationsverbünden angelegt werden kann, ist es möglich, diese Anschaffung auch parallel in anderen Bereichen der kommunalen IT zu nutzen. Darüber hinaus stellt das BSI eine Reihe von Grundschutztools auf seiner Webseite zur Verfügung[16].

[16] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/Alternative-IT-Grundschutztools/alternative-it-grundschutztools_node.html, abgerufen am 18. November 2022.

4 Erste Handlungsempfehlungen bei Störungen und Angriffen

Das Ziel des Informationssicherheitsmanagements ist es, die Informationen und Komponenten des Informationsverbundes vor Risiken und elementaren Gefährdungen zu schützen. Im Idealfall verhindern die Umsetzung von Maßnahmen und Einhaltung von Anforderungen bereits das Eintreten von Störungen oder einen Angriff. Dennoch lassen die in der Einleitung genannten Sicherheitsvorfälle und Attacken vermuten, dass auch Schulen in Zukunft immer stärker zu Angriffspunkten für Cyberangriffe werden. Diese eher „kleinen Kunden" anzugreifen und gegebenenfalls zu erpressen, wird wirtschaftlich immer interessanter für potenzielle Angreifende. Dies liegt einerseits an der wachsenden Anzahl an IT-Komponenten und andererseits an den technischen Möglichkeiten, Schwachstellen durch leistungsstarke IT-Systeme automatisiert zu finden und auszunutzen. Deshalb ist es die Pflicht aller Verantwortlichen im Schulbetrieb, einen Plan für IT-Sicherheitsnotfälle zu erarbeiten, um schnell und koordiniert reagieren zu können.

Prinzipiell kann von zwei grundlegenden Angriffsarten ausgegangen werden – dem Angriff von außen und dem von innen. Angriffe von außen bedeuten, dass mittels technischer Hilfsmittel Lücken gefunden oder erreichbare IT-Komponenten gestört werden. Erreichbar sind dabei beispielweise Internetzugangsgeräte (z. B. Router oder Firewall) oder ein Mailserver. Lücken sind dann Schwachstellen in der Software, die einem Angreifenden unautorisierten Zugriff, Zugang oder Zutritt zu IT-Systemen und deren Daten ermöglichen.

Angriffe von innen beziehen sich dagegen auf den nachlässigen Umgang von Nutzerinnen und Nutzern mit einer IT-Komponente, was dazu führt, dass ein Zugang oder Zutritt zu internen Systemen und damit der Zugriff auf geschützte Daten und Informationen für Dritte möglich wird. Das kann zum Beispiel eine E-Mail sein, die einen Schadcode enthält oder diesen nachlädt. Durch das unbedachte Öffnen der E-Mail wird ein (kleines) Programm im schulischen Netz installiert, das dann „von innen" Kontakt zu einem fremden Server aufnimmt und diesem wiederum den Zugriff auf und Zugang zum Schulnetz gewährt.

Im Falle eines Informationssicherheitsvorfalls in Schulen oder beim Schulträger sind zunächst folgende allgemeine Empfehlungen zu berücksichtigen:

Empfehlung 1: Externe Unterstützung

Auch wenn damit unter Umständen die Expertise der operativen Schuladministratoren und -administratorinnen infrage gestellt wird: Angriffe auf die IT-Infrastruktur einer Schule oder eines Schulträgers können selten von einer Person allein bewältigt werden. Wenden Sie sich daher an Expertinnen und Experten eines regionalen IT-Dienstleistungsunternehmen, die im Notfall schnell vor Ort sind.

Empfehlung 2: **Bestimmen von Verantwortlichen, die beim Eintreten eines Notfalls die Entscheidung zur Abschottung treffen dürfen**

Um die Ausbreitung des Schadens oder den Abfluss von Daten zu stoppen[17], ist es ein gängiger Ansatz, sofort „die Stecker" zu ziehen. Diese Entscheidung ist bewusst und umgehend zu treffen. Wer diese Entscheidung im Notfall treffen darf, muss im Vorfeld festgelegt und fixiert werden. Der Personenkreis sollte nicht zu klein sein, da jederzeit und möglichst schnell auf einen Notfall reagiert werden muss. Je nach Organisation kann dies die Schulleitung sein, aber auch eine erfahrene IT-Leitung oder IT-Administratorin, der

[17] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/Qualifizierung/Vorfall_Praktiker/Vorfall_Praktiker.html, abgerufen am 18. November2022.

oder die notwendigen Handlungen initiiert. Wichtig ist, dass es mehrere Entscheidungsträger und -trägerinnen mit gleichen Befugnissen ausgestattet sind, so dass zu jeder Zeit mindestens eine Person erreichbar ist.

Empfehlung 3: **Den Angriff dem regional zuständigen CERT und dem BSI melden**

Um eine kompetente Unterstützung und wertvolle Ratschläge zu erhalten, ist es sinnvoll, mit dem BSI Kontakt aufzunehmen und Sicherheitsvorfälle sowie Cyberangriffe zu melden. Auch Sicherheitslücken und Schwachstellen in IT-Produkten können und sollten der Meldestelle für Cybersicherheit mitgeteilt werden. Eine Unterstützung seitens des regional zuständigen CERT oder des BSI kann angefordert werden.

Weiterführende Informationen und Hinweise sowie Handlungsempfehlungen für Maßnahmen zur schnellen Absicherung schulischer IT-Systeme durch Umsetzungsverantwortliche finden Sie in der Handreichung „Informationssicherheit Schule im IT-Betrieb: Erste Schritte".

Diese Handlungsempfehlungen stellen keine erschöpfende Liste dar. Dennoch helfen Sie, erste Maßnahmen einzuleiten und Vorkehrungen zu treffen, um auf Störungen und Angriffe organisiert reagieren und im Ernstfall auf externe Unterstützung zurückgreifen zu können.

5 Glossar

Glossar	
Asset Management	Allgemein bezeichnet man mit Assets Vermögenswerte in einer Organisation. IT-Assets umfassen sowohl die Hardwarekomponenten als auch die eingesetzte Software in einer Organisation. Das Asset Management ist dafür verantwortlich, die Assets einer Organisation zu dokumentieren, bereitzustellen, zu warten, aktualisieren und stillzulegen, wenn der Zeitpunkt dafür gekommen ist.
Bedrohungen	Bedrohungen sind mögliche Ereignisse, die bei ihrem Eintritt einen Schaden auslösen können. Menschliches Fehlverhalten, technisches Versagen, höhere Gewalt oder organisatorische Mängel liegen Bedrohungen zugrunde.
Datensicherheit	Im Gegensatz zum Datenschutz und zur IT-Sicherheit befasst sich das Thema Datensicherheit mit dem generellen Schutz sämtlicher Daten in einer Organisation. Die Datensicherheit verfolgt also das Ziel, Daten jeglicher Art – also neben digitalen Daten auch Ausdrucke und Listen – gegen Bedrohungen, Manipulationen und unberechtigtem Zugriff abzusichern. Dabei werden die notwendigen Maßnahmen ergriffen, um die Sicherheit von Daten zu gewährleisten. Ziel der Datensicherheit ist es, Daten jeglicher Art zu schützen. Im Bundesdatenschutzgesetz (§ 48 BDSG) wird dieser Begriff im Zusammenhang mit der Verarbeitung besonderer Kategorien personenbezogener Daten genannt.
Datenschutz	Die unterschiedlichen Datenschutzregelungen des Bundes und der Länder definieren primär den Schutz der persönlichen Daten von natürlichen Personen sowie das Recht auf informationelle Selbstbestimmung. Darin wird in vielen Fällen die Frage beantwortet, ob Daten erhoben werden dürfen. Im Gegensatz zur Informationssicherheit ist der Datenschutz europaweit in der DSGVO sowie in landesspezifischen Gesetzen, Richtlinien und Verordnungen verankert.
Gefährdungen	Eine Gefährdung tritt immer dann ein, wenn eine Bedrohung auf eine Schwachstelle trifft.
Informationssicherheit	Die Informationssicherheit umfasst den Schutz sämtlicher Informationswerte in einem Informationsverbund. Der Informationsverbund kann die gesamte Institution beinhalten – den Schulträger mit den dazugehörigen Schulen oder aber nur klar definierbare Teilbereiche. Dies bedeutet, dass zum Beispiel zunächst erst einmal eine Schule betrachtet und als Informationsverbund festgelegt wird. Zu einem Informationsverbund gehören dann alle Objekte, die relevante Teile der Schul-IT sind. Dies sind sowohl (1) Räume, inklusive häusliche Arbeitsplätze, (2) IT-Systeme wie Server, stationäre und mobile Endgeräte und (3) Netze, zum Beispiel WLAN-Netze, Firewalls, Router sowie (4) Anwendungen wie Office Produkte oder Dateiablagen. Informationswerte sind dabei alle Daten in digitaler (Dateien) und materieller Form (z. B. Ausdrucke oder handschriftliche Notizen) sowie das Know-how der Mitarbeitenden. Damit schließt die Informationssicherheit sowohl die Felder Datensicherheit, IT-Sicherheit wie auch einen großen Teil des Datenschutzes mit ein. Die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität müssen jederzeit gewährleistet werden und sind ebenso für alle die Informationssicherheit tangierenden Bereiche gültig. Zum gegenwärtigen Zeitpunkt existiert keine gesetzliche Regelung zum Thema.
Integrität	Die Integrität ist ein Schutzziel der Informationssicherheit: Die Sicherstellung, dass Daten korrekt, vollständig und unversehrt sind. Änderungen von Daten müssen eindeutig nachvollziehbar sein.

Glossar

IT-Architektur	Unter IT- Architektur wird die gesamte IT-Infrastruktur, das IT-Management und die IT-Schnittstellen zusammengefasst. Sie beschreibt die jeweiligen Anwendungs-, Infrastruktur-, Informations- und Datenarchitekturen und deren Beziehungen untereinander.
IT-Beauftragte / IT-Beauftragter	Teilweise wird der/die Medienbeauftragte auch als IT-Beauftragte bzw. IT-Beauftragter bezeichnet. Davon sollte im Sinne einer möglichst scharfen Trennung von Rollen und Begrifflichkeiten Abstand genommen werden. Der Begriff des oder der IT-Beauftragten wird in diesem Dokument deshalb nicht verwendet.
IT-Governance	In der Regel besteht die IT-Governance aus einer klaren Führungsebene, Organisationsstrukturen und Prozessen beziehungsweise definierten Abläufen. Diese tragen gemeinsam die Verantwortung, dass die gesamte IT-Infrastruktur die Organisationsziele unterstützt.
IT-Sicherheit	Die IT-Sicherheit umfasst den Schutz von Informationswerten und IT-Systemen unter Einsatz von Informationstechnik. Der Fokus liegt auf dem Schutz sämtlicher elektronisch gespeicherter Informationen und deren Verarbeitung mithilfe technischer Systeme.
Problem Management	Innerhalb des IT-Services steuert das Problem Management die Behebung von IT-Störungen und untersucht deren Ursache. Es führt standardisierte Vorgehensweisen ein, um die Abläufe der IT-Prozesse zu analysieren und eine schnelle Wiederherstellung der Dienste nach einem Ausfall zu gewährleisten.
Schwachstellen	Schwachstellen werden definiert als Schwächen der Sicherheitsmaßnahmen oder der Informationswerte. Dies können zum Beispiel schlecht geschützte Firewalls aber auch Passwörter auf Klebezetteln am Bildschirm sein.
Service Desk	Unter Service Desk versteht man in der Regel den IT-Service, der für alle Beteiligten einer Organisation erreichbar ist und Lösungen findet, wenn etwas bei der IT nicht funktioniert.
Verfügbarkeit	Die Verfügbarkeit Schutzziel der Informationssicherheit: Die Sicherstellung, dass Daten in den zuvor festgelegten Zeiträumen zur Verfügung stehen.
Vertraulichkeit	Die Vertraulichkeit ist ein Schutzziel der Informationssicherheit: Der Zugriff, das Lesen und die Übermittlung von Daten dürfen nur von zuvor autorisierten Nutzerinnen und Nutzern durchgeführt werden.

6 Abkürzungsverzeichnis

Abkürzungsverzeichnis	
APP	Applications / Anwendungen
APT	Advanced Persistent Threats (zielgerichtete, effektive Cyberangriffe)
BSI	Bundesamt für Sicherheit in der Informationstechnik
CD ROM	Compact Disc Read-Only Memory (Permanentspeichermedium für digitale Daten)
CERT	Computer Emergency Response Teams (Computersicherheits-Ereignis- und Reaktionsteam)
CON	Konzepte und Vorgehensweise
DER	Detektion und Reaktion
DSGVO	Datenschutz-Grundverordnung
DVD	Digital Versatile Disc (digitaler, optischer Datenspeicher; ursprünglich Digital Video Disc)
INF	Infrastruktur
IKT	Informations- und Kommunikationstechnik
ISMS	Informationssicherheitsmanagementsystem (Englisch: Information Security Management System)
ISO	Internationale Organisation für Normung
IT	Informationstechnik
MDM	Mobile-Device-Management (Verwaltung mobiler Endgeräte)
NET	Netze und Kommunikation
OPS	Betrieb
ORP	Organisation und Personal
SYS	IT-Systeme
USB	Universal Serial Bus (bit-serielles Datenübertragungssystem)
USV	Unterbrechungsfreie Stromversorgung
BSI 200-2	BSI IT-Grundschutz-Methodik
CISIS 12	Informationssicherheitsmanagementsystem (ISMS) in 12 Schritten
ISO 27001	Internationaler Standard für ein Informationssicherheitssystem (ISMS)
VdS 1000	Maßnahmenkatalog für ISMS

7 Autorinnen und Autoren

Uta Fiedler

Dr. Michael Krause

Maleika Krüger

Mathias Ragnow

Antje Reuter

Für ihre Unterstützung bedanken wir uns bei SONOXO.AI-GmbH&Co.KG:

Astrid Aha

Alexander Gutendorf

Wir danken der Unterstützung durch den ITV.SH.

Kontakt:

PD – Berater der öffentlichen Hand GmbH

Friedrichstr. 149

10117 Berlin

pd-g.de/

Email: SchuleDigital@pd-g.de

Die vorliegende Handreichung im Modul "IT-Steuerung und Kooperation" wurde im Rahmen einer Ressortforschung des Bundesministeriums der Finanzen (BMF), finanziert aus Mitteln des Deutschen Aufbau- und Resilienzplans (DARP), erstellt.

Finanziert von der Europäischen Union
NextGenerationEU

8 Quellen

Arbeitsgruppe Kommunale Basis-Absicherung [AG KOBA] (2022): IT-Grundschutz-Profil Basis-Absicherung Kommunalverwaltung, https://www.landkreistag.de/images/stories/themen/egovernment/220331_IT-Grundschutz-Profil.pdf, abgerufen am 23. November 2022.

Bundesamt für Sicherheit in der Informationstechnik [BSI] (2023): IT-Grundschutz-Kompendium, Reguvis Fachmedien GmbH, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4#download=1, abgerufen am 07.02.2023

Bundesamt für Sicherheit in der Informationstechnik [BSI] (2022b): Awareness, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Faktor-Mensch/Awareness/awareness_node.html, abgerufen am 14. September 2022.

Mitteldeutscher Rundfunk [MDR] (2022): „Hacker-Attacken in Deutschland. IT-Angriffe: Kleine Kommunen, große Gefahr.“, https://www.mdr.de/nachrichten/deutschland/gesellschaft/kommune-cyberangriff-it-sicherheit-sachsen-anhalt-thueringen-100.html, abgerufen am 23. November 2022.

Sicherheit für Kommunen in Schleswig-Holstein (SiKoSH): https://itvsh.de/sikosh/ , abgerufen am 22.03.2023.

Anhang A: Gefährdungen nach BSI

Dargestellt ist eine Zusammenfassung der elementaren Gefährdungen für Zielobjekte im Bereich der IT. Es sind dabei nicht alle Gefährdungen für jedes Zielobjekt relevant. So kann Wasser beispielsweise die Hardware-Komponenten an einem Standort beschädigen, bedroht aber nicht die Cloud-Lösungen, mit denen die Hardware verbunden ist, sofern diese an einem anderen Ort gehostet wird.

G 0.1 Feuer

Feuer verursacht direkte Schäden an Menschen, Gebäuden und Einrichtungen. Folgeschäden durch Löschwasser, Rauch und Gase – auch an nicht direkt vom Brand betroffenen Orten – sind möglich.

Mögliche Ursachen:
- Fahrlässiger Umgang mit Feuer
- Unsachgemäße Benutzung von Elektronik
- Technische Defekte

G 0.2 Ungünstige klimatische Bedingungen

Hitze, Frost, Luftfeuchtigkeit und häufige klimatische Schwankungen können zu Schäden an der Technik führen und Arbeitsunfähigkeit, Verletzung oder den Tod von Menschen zur Folge haben.

Mögliche Ursachen:
- Fehlende oder defekte Klimaanlage
- Fehlende Heizung
- Zu feuchte Räumlichkeiten

G 0.3 Wasser

Wasser kann zu Schäden an technischen Komponenten führen. Mögliche Folgen sind Kurzschlüsse, mechanische Beschädigung, Rost und Frost.

Mögliche Ursachen:
- Störungen in der Wasserver- oder Abwasserentsorgung
- Defekte Heizungsanlage
- Defekte Sprinkleranlage
- Löschwasser bei der Brandbekämpfung
- Sabotage

G 0.4 Verschmutzung, Staub, Korrosion

Mechanische Komponenten sind störungsanfällig für geringe Mengen an Staub und Verschmutzungen. Das kann zu Ausfällen oder Beschädigungen von IT-Komponenten und Versorgungseinrichtungen führen. Um dies zu verhindern, gibt es oft Sicherheitsabschaltungen in den Geräten.

Mögliche Ursachen:
- Arbeiten an Wänden oder anderen Gebäudeteilen
- Umrüstungsarbeiten an der Hardware
- Auspacken von Geräten

G 0.5 Naturkatastrophen

Naturkatastrophen können Beschädigungen an technischen Einrichtungen und Gebäuden hervorrufen sowie zu Verletzungen oder den Tod von Menschen führen. Die Höhe des Risikos ist stark standortabhängig und betrifft gelegentlich auch den Ausfall von wichtigen Versorgungseinrichtungen.

Mögliche Ursachen:
- Erdbeben
- Hochwasser
- Erdrutsche
- Tsunamis
- Lawinen
- Vulkanausbrüche

G 0.6 Katastrophen im Umfeld

Das sind Gefahren durch Unglücksfälle mit Bränden, Explosionen, der Freisetzung giftiger Substanzen oder dem Austreten gefährlicher Strahlung und sich daran anschließender Aktivitäten wie zum Beispiel Sperrungen. Mögliche Gefahren aus dem Umfeld sind der Verkehr, Nachbarbetriebe oder Wohngebiete.

G 0.7 Großereignisse im Umfeld

Die Gefahr durch Behinderungen des ordnungsgemäßen Betriebs entsteht zum Beispiel durch Straßenfeste, Konzerte, Sportveranstaltungen oder Demonstrationen. Zusätzliche Gefahren bei Ausschreitungen sind die Einschüchterung von Mitarbeitenden und Gewaltanwendung gegen Personal oder Gebäude.

G 0.8 Ausfall oder Störung der Stromversorgung

Abschaltungen und Unterbrechungen der Stromversorgung seitens der Verteilungsnetzbetreiber können den IT-Betrieb stören. Dies betrifft neben der IT auch Infrastruktur-Einrichtungen wie Aufzüge, Klimatechnik, Gefahrenmeldeanlagen und automatische Türschließanlagen.

G 0.9 Ausfall oder Störung von Kommunikationsnetzen

Der Ausfall oder die Störung von Telefon, Fax, E-Mai oder dem Internet über einen längeren Zeitraum führt dazu, dass Geschäftsprozesse nicht mehr weiterbearbeitet werden, Kunden die Institution nicht mehr erreichen und Aufträge nicht abgegeben oder beendet werden können.

G 0.10 Ausfall oder Störung von Versorgungsnetzen

Die Versorgungsnetze sind in unterschiedlichem Maße voneinander abhängig.
Ausfälle oder Störungen führen möglicherweise zu einer Beeinträchtigung des IT-Betriebs oder der Arbeitsfähigkeit des Personals. Beispiele wichtiger Versorgungsnetze sind Strom, Telefon, Kühlung, Heizung bzw. Lüftung, Wasser und Abwasser, Löschwasserspeisungen sowie Melde- und Steueranlagen.

G 0.11 Ausfall oder Störung bei Dienstleistungsunternehmen

Durch Ausfälle von externen Dienstleistungen kann die Aufgabenbewältigung und die betriebliche Kontinuität beeinträchtigt werden. Gleiches gilt für Unterauftragnehmerinnen bzw. Unterauftragnehmer des Dienstleistungsunternehmens.

Mögliche Ursachen:
- Insolvenz
- Einseitige Kündigung des Vertrags
- Betriebliche Probleme

- Personalausfall
- Störungen der IT-Systeme
- Mangelhafte Leistungen

G 0.12 Elektromagnetische Störstrahlung

Elektronische Komponenten sind anfällig für elektromagnetische Störstrahlung. Die Folgen sind Ausfälle, Störungen, falsche Verarbeitungsergebnisse oder Kommunikationsfehler. Bei drahtloser Kommunikation sind die Frequenzbänder anfällig und bei Datenträgern können Informationen durch elektromagnetische Strahlung gelöscht oder verfälscht werden.

Mögliche Ursachen:
- Funknetze
- Dauermagneten
- Kosmische Strahlung
- Elektrische Geräte

G 0.13 Abfangen kompromittierender Strahlung

Elektrische Geräte strahlen elektromagnetische Wellen ab, diese können Daten enthalten, die in näherer Umgebung abgefangen und rekonstruiert werden können. Auch bei Schallwellen besteht das Risiko, dass sie abgefangen werden, um Informationen zu erlangen.

G 0.14 Ausspähen von Informationen (Spionage)

Dies wird unter anderem genutzt, um Wettbewerbsvorteile zu erlangen, Personen zu erpressen oder ein Produkt nachbauen zu können. Es gibt technische, optische, akustische und elektronische Methoden des Ausspähens. Darüber hinaus können auch öffentlich zugänglichen Quellen zusammengeführt werden.

G 0.15 Abhören

Das ist eine Aufwand-Nutzen-Rechnung für die Angreifenden. Die Methoden reichen vom Belauschen bis zum technischen Abfangen von Signalen. Das Risiko, entdeckt zu werden, ist gering. Es gibt keine wirklich abhörsicheren Kabel, besonders gefährdet sind Klartextprotokolle wie HTTP.

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

Der Schaden besteht hier aus der Offenlegung vertraulicher Informationen, dem Verlust von Kunden und den Kosten für die Wiederbeschaffung und Wiederherstellung eines arbeitsfähigen Zustandes. Betroffen sind unter anderem Server, mobile Geräte und USB-Sticks.

G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten

Es entsteht ein Mangel an Verfügbarkeit, Kosten durch die Neubeschaffung und es droht die Offenlegung von vertraulichen Informationen. Beim Wiederauftauchen der Geräte, Datenträger oder Dokumente besteht das Risiko, dass unerwünschte Programme aufgespielt wurden.

G 0.18 Fehlplanung oder fehlende Anpassung

Sicherheitsprobleme entstehen bei nicht sachgerechter Gestaltung von organisatorischen Abläufen, nicht bedachten Abhängigkeiten in Prozessen, unklarer Aufgaben- und Verantwortungszuteilung und nicht sachgerechter Nutzung von Geräten und Verfahren. Bei Veränderungen (z. B. bei Mitarbeitenden, Hard- und Software) müssen notwendige organisatorische und technische Anpassungen vorgenommen werden.

G 0.19 Offenlegung schützenswerter Informationen

Mögliche Zugriffspunkte zur Erlangung vertraulicher Informationen sind unter anderem Festplatten, USB-Sticks, Ausdrucke/Akten und während der Datenübertragung. Der Zugriff kann unter anderem durch Diebstahl, unbedachte Weitergabe, unzureichende Vernichtung, Abhören oder Auslesen durch Schadprogramme erfolgen. Mögliche Folgen sind Gesetzesverstöße, negative Außen- und Innenwirkung und finanzieller Schaden.

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

Die Nutzung von Informationen und Produkten aus unzuverlässigen Quellen birgt das Risiko, dass falsche Daten als Basis für Entscheidungen oder Berechnungen genutzt werden. Außerdem ist dadurch die Integrität und Verfügbarkeit von IT-Systemen gefährdet.

G 0.21 Manipulation von Hard- oder Software

Dies kann unter anderem Geräte, Zubehör, Datenträger und Applikationen betreffen. Die Manipulation führt nicht immer zu unmittelbarem Schaden. Je später er entdeckt wird, umso größer ist der Schaden. Mögliche Schäden sind der Verlust von Vertraulichkeit, Integrität und Verfügbarkeit sowie die Zerstörung von Datenträgern oder IT-Systemen.

G 0.22 Manipulation von Informationen

Hier geht es um fehlerhaftes oder vorsätzlich falsches Erfassen oder Verändern von Daten. Wie schwerwiegend die Manipulation ist, ist abhängig von den Zugriffsmöglichkeiten, die eine Person auf Informationen hat.

G 0.23 Unbefugtes Eindringen in IT-Systeme

Jede Schnittstelle zu einem IT-System birgt das Risiko eines unbefugten Zugriffs.

G 0.24 Zerstörung von Geräten oder Datenträgern

Fahrlässigkeit, unsachgemäße Verwendung oder ungeschulten Umgang kann zur Zerstörung von Geräten und Datenträgern führen. Damit geht auch die Gefahr einher, dass Informationen verloren gehen.

G 0.25 Ausfall von Geräten oder Systemen

Bei zeitkritischen Anwendungen sind die Folgeschäden nach einem Systemausfall entsprechend hoch, wenn es keine Ausweichmöglichkeiten gibt.

G 0.26 Fehlfunktion von Geräten oder Systemen

Durch die Komplexität gibt es bei Soft- und Hardware viele unterschiedliche Fehlerquellen, die zu Fehlfunktionen und Sicherheitsproblemen führen können. Bleiben diese unentdeckt, kann dies zu Folgefehlern führen.

<u>Mögliche Ursachen</u>:
- Materialermüdung
- Überschreitung von Grenzwerten
- Fehlende Wartung

G 0.27 Ressourcenmangel

Der Mangel an personellen, zeitlichen, technischen und finanziellen Ressourcen kann zu Engpässen, Überlastungen und Ausfällen führen. Schon kleine Vorfälle können hierbei große Auswirkungen auf die Geschäftsprozesse haben.

G 0.28 Software-Schwachstellen oder -Fehler

Abstürze oder Fehler, die bei Anwendungen entstehen, können, wenn sie nicht rechtzeitig erkannt werden, zu weitreichenden Folgen führen, wie etwa zu Fehlern bei Berechnungsergebnissen, Fehlentscheidungen und Verzögerungen in Prozessen sowie Sicherheitslücken.

G 0.29 Verstoß gegen Gesetze oder Regelungen

Bei ungenügender Absicherung von Informationen, Prozessen und IT-Systemen kann es zu Verstößen gegen Rechtsvorschriften bei der Informationsverarbeitung oder gegen bestehende Verträge mit Geschäftspartnern kommen. Bei mehreren Standorten gilt es, gegebenenfalls unterschiedliche Gesetze zu beachten.

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

Bei IT-Systemen geht es hier insbesondere um die Identifikation und Authentisierung von berechtigten Benutzerinnen und Benutzern. Als Schutz dienen Zugriffs- und Zugangskontrollen. Die Folgen eines unberechtigten Zugriffs können Offenlegung von Informationen, Manipulationen und Störungen sein; insbesondere bei Administratorenrechten können dabei schwere Schäden entstehen.

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

Das Missachten oder Umgehen von Sicherheitsmaßnahmen kann zu Störungen oder Ausfällen führen. Bei fehlerhafter Bedienung von IT-Systemen oder Anwendungen können Daten versehentlich gelöscht oder verändert werden und vertrauliche Informationen an die Öffentlichkeit gelangen.

G 0.32 Missbrauch von Berechtigungen

Über Berechtigungen wird der Zugang zu Informationen gesteuert und kontrolliert. Oft verfügen Personen aus historischen, systemtechnischen oder anderen Gründen über umfangreichere Zutritts- oder Zugriffsrechte als sie für ihre Tätigkeit benötigen; diese Rechte können für Angriffe missbraucht werden.

G 0.33 Personalausfall

Es wird unterschieden in unvorhersehbaren und vorhersehbaren Personalausfall. Beides kann Einfluss auf die Organisation und die Geschäftsprozesse haben.

Mögliche unvorhersehbare Ursachen:
- Krankheit
- Interne Wechsel
- Unfall
- Tod
- Streik

Mögliche vorhersehbare Ursachen:
- Urlaub
- Fortbildung
- Vertragsablauf

G 0.34 Anschlag

Diese Gefährdung kann für eine ganze Institution, bestimmte Bereiche oder einzelne Personen bestehen. Die Höhe des Risikos für eine Institution hängt von der Lage des Gebäudes, dem Aufgabenfeld und vom politisch-sozialen Klima ab. Für die Einschätzung der Bedrohung beraten auf Anfrage die Landeskriminalämter und das Bundeskriminalamt.

G 0.35 Nötigung, Erpressung oder Korruption

Nötigung oder Korruption können alle Grundwerte der Informationssicherheit beeinträchtigen. Ziele sind unter anderem das Erlangen oder Manipulieren von Informationen oder die Störung von Geschäftsprozessen.

G 0.36 Identitätsdiebstahl

Hierfür werden personenbezogene Informationen wie Geburtsdatum, Anschrift, Kreditkarten- oder Kontonummern benötigt. Das Risiko ist bei geringer Identitätsprüfung in Verbindung mit teuren Dienstleistungen besonders hoch. Die Folgen bestehen oft aus Rufschädigung, finanziellem Schaden und einem hohen Zeitaufwand für die Aufklärung und Schadensbegrenzung.

G 0.37 Abstreiten von Handlungen

Neben Handlungen kann auch der Versand oder Empfang von Informationen verleugnet werden. Gründe hierfür sind unter anderem der Verstoß gegen Anweisungen, Sicherheitsvorgaben und Gesetze oder das Vergessen eines Termins. Im Bereich der Informationssicherheit wird häufig die Verbindlichkeit betont; dadurch soll sichergestellt werden, dass erfolgte Handlungen nicht unberechtigt abgestritten werden können.

G 0.38 Missbrauch personenbezogener Daten

Der Missbrauch kann zur Beeinträchtigung der gesellschaftlichen Stellung oder wirtschaftlichen Verhältnisse einer Person führen. Ein Missbrauch liegt zum Beispiel vor, wenn zu viele Daten gesammelt werden, es keine Einwilligung gibt, die Daten nicht rechtzeitig gelöscht oder zweckentfremdet werden.

G 0.39 Schadprogramme

Es handelt sich dabei um Software, die ohne Wissen oder Einwilligung der Nutzerin bzw. des Nutzers schädliche Funktionen ausführt. Die Möglichkeiten reichen von der Datenauslese bis zur Systemfernsteuerung. Dadurch können Informationen verfälscht werden oder verlorengehen, ferner können Imageverlust und finanzieller Schaden daraus resultieren.

G 0.40 Verhinderung von Diensten (Denial of Service)

Das sind Angriffsformen (auch DoS-Angriff genannt), die mit dem Ziel durchgeführt werden, die vorgesehene Nutzung von Dienstleistungen, Funktionen oder Geräten zu verhindern, zum Beispiel durch das verursachen von IT-Ausfällen. Dabei werden meistens die Ressourcen einer Institution durch den/die Angreifenden überbeansprucht, damit sie für die eigentlichen Nutzerinnen und Nutzer nicht mehr zugänglich sind.

G 0.41 Sabotage

Diese mutwillige Manipulation oder Beschädigung von Sachen oder Prozessen erfolgt überwiegend durch interne Täter. Häufige Ziele sind Rechenzentren oder Kommunikationsanbindungen, diese werden insbesondere über unzureichend geschützte Infrastruktur punktuell manipuliert.

G 0.42 Social Engineering

Hierbei werden menschliche Eigenschaften wie Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt. Eine oft genutzte Methode sind Telefonanrufe unter Vortäuschung falscher Autorität oder Zugehörigkeit, um Passwörter oder Ähnliches zu erlangen. Auch mehrstufige Angriffe über einen längeren Zeitraum sind möglich.

G 0.43 Einspielen von Nachrichten

Angreifende senden speziell vorbereitete Nachrichten mit dem Ziel, für sich selbst einen Vorteil oder einen Schaden für das Opfer zu erreichen. Für die Konstruktion werden zum Beispiel Protokollspezifikationen oder Aufzeichnungen über das Kommunikationsverhalten in der Vergangenheit genutzt.

G 0.44 Unbefugtes Eindringen in Räumlichkeiten

Die mit dem Eindringen verbundenen Gefahren sind der Diebstahl und die Manipulation von Informationen oder IT-Systemen. Daneben sind Sachschäden an Eingängen und Geräten möglich.

G 0.45 Datenverlust

Häufig werden Daten unbeabsichtigt oder unerlaubt gelöscht, zum Beispiel durch Fehlbedienung, Fehlfunktionen, Stromausfälle, Verschmutzung oder Schadsoftware. Ein Datenverlust kann jedoch auch durch Beschädigung und Diebstahl von Geräten oder Datenträgern entstehen oder durch Unachtsamkeit bei der Synchronisierung von Geräten.

G 0.46 Integritätsverlust schützenswerter Informationen

Mögliche Folgen des Integritätsverlustes sind, dass Informationen nicht mehr lesbar sind oder nicht mehr entschlüsselt werden können. Verfälschte Daten führen dazu, dass falsche Informationen weitergegeben werden. Elektronische Dokumente verlieren an Beweiskraft, wenn ihre Integrität nicht nachgewiesen werden kann.

Mögliche Ursachen:
- Manipulationen
- Fehlverhalten
- Fehlbedienung
- Fehlfunktionen
- Übermittlungsfehler

G 0.47 Schädliche Nebeneffekte IT-gestützter Angriffe

Diese Nebeneffekte treten aufgrund der hohen Komplexität und Vernetzung moderner Informationstechnik auf und können von den Tätern unbeabsichtigt sein, andere Objekte betreffen oder Unbeteiligte schädigen.

Anhang B: Quick-Check-Bögen (BSI-Basis-Absicherung) für Schulen und Schulträger

Hinweis zur Anwendung: Durch Doppelklick auf die Quick-Checks öffnen diese in Excel.