IDR Prüfungsleitlinie IDR-L 113-1 „Informationssicherheit“

Stand: 09.2023

Autoren:

Alexander Ehrbar; Gemeindeprüfungsanstalt Nordrhein-Westfalen

Ralf Klomfaß; Revisionsamt Landeshauptstadt Mainz

Matthias Warnecke, LWL-Rechnungsprüfungsamt

Inhalt

I. Abbildungsverzeichnis

Es konnten keine Einträge für ein Abbildungsverzeichnis gefunden werden.

II. Dokumentenhistorie

Version	Datum	Verfasser	Änderung / Grund	Status
01.0	2022	Alexander Ehrbar Ralf Klomfaß	Erstellung des Dokuments	In Arbeit
01.0	12.2022	AK DITS	Vorstellung / Sichtung im AK	ENTWURF
01.0	09.2023	AK DITS	Einarbeitung redaktioneller Anmerkungen	FINAL

2. Anforderungen an die IT- Sicherheit

2.1. Zielsetzung

Mit der Digitalisierung in Behörden ist auch die Anhängigkeit von funktionierenden IT-Systemen gestiegen. Die Betriebsbereitschaft und Sicherheit der IT- Systeme ist nunmehr auch für die öffentliche Verwaltung von existenzieller Bedeutung geworden. Ziel der Betrachtung der IT-Sicherheit ist die Ermittlung des Sicherheitsniveaus im Bereich der Informationstechnik. Diese Untersuchung umfasst sowohl technische als auch organisatorische Maßnahmen für ein angemessenes Sicherheitsniveau und soll Schwachstellen und Handlungsbedarfe aufzeigen.

2.2. Rechtsgrundlagen

- BSI- Grundschutzkompendium

3. Erläuterung/Grundinformation

Informationen sind ein wesentlicher Wert für Behörden und müssen daher angemessen geschützt werden. Die meisten Geschäftsprozesse und Fachaufgaben sind heute in der Verwaltung ohne IT-Unterstützung längst nicht mehr vorstellbar. Eine zuverlässig funktionierende Informationsverarbeitung ist ebenso wie die zugehörige Technik für die Aufrechterhaltung des Betriebes unerlässlich.

Mit dem IT-Grundschutz bietet das BSI eine praktikable Methode an, um die Informationen einer Institution angemessenen zu schützen. Als IT-Grundschutz bezeichnet das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Vorgehensweise zum Identifizieren und Umsetzen von Sicherheitsmaßnahmen der unternehmenseigenen Informationstechnik (IT). Das Ziel des Grundschutzes ist das Erreichen eines mittleren, angemessenen und ausreichenden Schutzniveaus für IT-Systeme. Zum Erreichen des Ziels empfiehlt das IT-Grundschutz-Kompendium (vormals: IT-Grundschutz-Kataloge) technische Sicherheitsmaßnahmen und infrastrukturelle, organisatorische und personelle Schutzmaßnahmen.

3.1. In welchen Bereichen können Schäden auftreten?

Potentielle Schäden durch Mängel im Bereich des IT- Grundschutzes lassen sich folgenden Kategorien zuordnen:

- **Verlust der Verfügbarkeit**: wenn grundlegende Informationen nicht vorhanden sind, fällt dies meistens schnell auf, vor allem, wenn Aufgaben ohne diese nicht weitergeführt werden können. Funktioniert ein IT-System nicht, können beispielsweise keine Geldtransaktionen durchgeführt werden, Online-Bestellungen sind nicht möglich, Produktionsprozesse stehen still. Auch wenn die Verfügbarkeit von bestimmten Informationen lediglich eingeschränkt ist, können die Geschäftsprozesse bzw. Fachaufgaben einer Institution beeinträchtigt werden.
- **Verlust der Vertraulichkeit von Informationen**: jeder Bürger und jeder Kunde möchte, dass mit seinen personenbezogenen Daten vertraulich umgegangen wird. Jedes Unternehmen sollte wissen, dass interne, vertrauliche Daten über Umsatz, Marketing, Forschung und Entwicklung die Konkurrenz interessieren. Die ungewollte Offenlegung von Informationen kann in vielen Bereichen schwere Schäden nach sich ziehen.
- **Verlust der Integrität (Korrektheit) von Informationen:** gefälschte oder verfälschte Daten können beispielsweise zu Fehlbuchungen, falschen Lieferungen oder fehlerhaften Produkten führen. Auch der Verlust der Authentizität (Echtheit und Überprüfbarkeit) hat, als ein Teilbereich der Integrität, eine hohe Bedeutung. Daten werden beispielsweise einer falschen Person zugeordnet. So können Zahlungsanweisungen oder Bestellungen zu Lasten einer dritten Person verarbeitet werden, ungesicherte digitale Willenserklärungen können falschen Personen zugerechnet werden, die „digitale Identität“ wird gefälscht[1].

Im IT-Grundschutz-Kompendium werden standardisierte Sicherheitsanforderungen für typische Geschäftsprozesse, Anwendungen, IT-Systeme, Kommunikations-verbindungen und Räume in IT-Grundschutz-Bausteinen beschrieben.

Ziel des IT-Grundschutzes ist es, einen angemessenen Schutz für alle Informationen einer Institution zu erreichen.

[1] IT-Grundschutz-Kompendium, Stand Februar 2022

4. Checkliste

Das IT- Grundschutzkompendium besteht in der aktuellen Fassung aus einem rund 900 Seiten umfassenden Gesamtwerk. Es ist nicht Aufgabe der Rechnungsprüfung, eine Umsetzungsprüfung der Grundschutzmaßnahmen des Grundschutzkatalogs durchzuführen. Vielmehr geht es darum, im Sinne eines systemischen Ansatzes zu prüfen, ob die IT- Verantwortlichen die wesentlichen Bausteine des Grundschutzes betrachtet und elementare Maßnahmen technischer und organisatorischer Art initiiert haben. Eine tiefgreifende Kenntnis von IT- Systemen ist dafür nicht erforderlich.

Lfd. Nr.	Soll-Vorgabe / Best-Practice-Empfehlung	Prüffrage	Zusatzinformationen
1	Technikräume	1. Besteht eine Zertifizierung für den Serverraum? Falls ja, bitte erläutern um welche Zertifizierung es sich handelt (TÜV, BSI etc.) und in welchem Jahr diese durchgeführt wurde? 2. Sind die Stromkreise für die Hardware, Stromversorgung und für sonstige Verbraucher (Licht, allgemeine Steckdosen etc.) voneinander getrennt? 3. Gibt es in direkter Nähe zur Zugangstür zum Serverraum (innen oder außen) einen Handfeuerlöscher?	BSI- Zertifizierung, physische Sicherheit von Serverräumen und Technikräumen, Redundanz, Zutrittsberechtigung, vorbeugender Brandschutz

		4. Wird im Zugang zum Serverraum eine sicherheitszertifizierte Tür verwendet? Falls ja, bitte WK- und Feuerwiderstandsklasse nennen. 5. Sind im Serverraum Fenster vorhanden? Falls Fenster vorhanden sind, wie wird gewährleistet, dass diese dauerhaft geschlossen sind? 6. Welche Art von Gefahrenmeldern werden eingesetzt? (Einbruch, Brand, Rauch, Wärme etc.) 7. Wie ist die Meldekette im Fall der Alarmierung organisiert? 8. Sind die Türen zum Serverraum immer verschlossen? Falls ja, wie wird dies gewährleistet? Zum Beispiel automatisches Zufallen der Tür und Öffnung nur per Schlüssel\Button. 9. Sind im Serverraum wasserführende Leitungen? Unvermeidbare Leitungen z.B. die einer Klimaanlage sind hier nicht gemeint. 10. Sollten wasserführende Leitungen vorhanden sein, wurden entsprechende Maßnahmen zur Vermeidung von Wasserschäden getroffen? Dies könnten zum Beispiel Ableitbleche, zusätzliche wasserdichte Ummantelungen, Leckage-Sensoren, zusätzliche regelmäßige Begehungen zur Begutachtung von	

		Korrosion etc. sein. Insbesondere bei der Auswahl "teilweise" bitte nähere Erläuterungen hierzu in der entsprechenden Spalte. 11. Wurden Maßnahmen zum Schutz vor Blitzschäden getroffen? Hier sind weitere Maßnahmen gemeint, die über den Schutz durch mögliche USVen (Unterbrechungsfreie Stromversorgung) hinausgehen. 12. Gibt es eine Netzersatzanlage? 13. Falls es eine Netzersatzanlage gibt, werden regelmäßige Tests durchgeführt, ob die Anlage betriebsbereit ist? 14. Ist die Klimatisierung im Serverraum redundant ausgelegt? 15. Werden USVen eingesetzt? 16. Falls USVen eingesetzt werden, werden regelmäßige Wartungen durchgeführt? 17. Gibt es USVen für alle Bereiche des Serverraums? Bei der Auswahl "nein" bitte nähere Erläuterungen in der entsprechenden Spalte. 18. Für welchen Betriebszeitraum genügt die Leistung der USVen?	

		19. Erfolgt eine Störungsmeldung für Server, Netzwerkkomponenten, Storage etc. innerhalb der gewöhnlichen Dienstzeiten? Falls ja, bitte näher erläutern wie diese erfolgt, z.B. Monitoring o.ä.. 20. Erfolgt eine Störungsmeldung für Server, Netzwerkkomponenten, Storage etc. außerhalb der gewöhnlichen Dienstzeiten? Falls ja, bitte näher erläutern wie diese erfolgt, z.B. Meldung auf Handy der IT-Mitarbeiter/innen mit Bereitschaft o.ä.. 21. Sind in der technischen Infrastruktur alle Komponenten redundant ausgelegt? Gemeint sind hier alle Bauteile vom Serverraum bis zum Nutzer also z.B.: Core-Switch, Server, Teilnehmeranschluss, Firewall, Switche, etc. 22. Sollten nicht alle Komponenten redundant ausgelegt sein, besteht für die übrigen Komponenten eine Standby Redundanz bzw. entsprechende Verträge die einen Ersatz in angemessener Zeit gewährleisten? 23. Gibt es formelle Regelungen, in denen die wichtigsten Anforderungen, die an einen Serverraum zu stellen sind, grundsätzlich dokumentiert sind (z.B.	

		Raumplanungskonzept mit grober Definition der Anforderungen)? 24. Wird auf die Einhaltung der Brandschutzvorschriften geachtet? Dies betrifft zum Beispiel die Kennzeichnung und das Freihalten von Fluchtwegen, das Verkeilen von Brandschutztüren etc. 25. Wird das Betreten des Raumes durch technische Maßnahmen erfasst und personenscharf zugeordnet? 26. Gibt es eine manuelle Dokumentation für Dritte die den Serverraum betreten? 27. Wird darauf geachtet, dass sich im Serverraum keine Brandlasten befinden? 28. Werden hochverfügbare Architekturen verwendet? Dies ist gegeben, wenn die Ausfallzeit pro Monat maximal rund fünf Minuten beträgt. 29. Falls Sie eine eigene Datenhaltung betreiben, ist das Storage System redundant ausgelegt? 30. Kommt eine Virtualisierung zum Einsatz? Falls ja, nennen Sie bitte die eingesetzte Software in den Erläuterungen.	

2	Sicherheitsmanagement / Sicherheitsorganisation	31. Wurde eine Leitlinie zur IT-Sicherheit verabschiedet? 32. Gibt es eine/n IT-Sicherheitsbeauftragte/n? Falls ja, wo ist diese/r organisatorisch angesiedelt? 33. Wie ist das IT-Sicherheitsmanagement ansonsten organisiert? Gibt es zum Beispiel dezentrale Ansprechpartner o.ä.? 34. Wurde ein formelles IT-Sicherheitskonzept verabschiedet? 35. Werden regelmäßig Management-Berichte zur Informationssicherheit erstellt? 36. Gibt es eine Dokumentation des Sicherheitsprozesses? In diesem sollte zum Beispiel die Zuständigkeiten bei Gefahrenpotentialen für bestimmte Zeiträume geregelt sein. 37. Gibt es eine Festlegung der Sicherheitsziele und -strategie? 38. Wurden für die unterschiedlichen Zielgruppen entsprechend angepasste Sicherheitsrichtlinien erstellt?	Sicherheitsleitlinie, Sicherheitskonzept, Sicherheitsbeauftragter

4	organisatorische Maßnahmen	39. Sind die Verantwortlichkeiten und Regelungen für den Einsatz in der IT-Stelle zum Beispiel durch Stellenbeschreibungen eindeutig geregelt? 40. Wer ist für die Vergabe der Zutrittsberechtigungen zum Serverraum verantwortlich? 41. Ist die Vergabe von Zutrittsberechtigungen in geeigneter Weise dokumentiert? Zum Beispiel in Form einer Dienstanweisung. 42. Wer ist für die Vergabe von Zugangsberechtigungen zu den verschiedenen Systemen verantwortlich? 43. Wer ist für die Vergabe von Zugriffsrechten innerhalb der einzelnen Applikationen verantwortlich? 44. Werden schützenswerte Betriebsmittel (Festplatten etc.) ordnungsgemäß entsorgt? 45. Ist die Schlüsselverwaltung in geeigneter Weise dokumentiert, z.B. in Form einer Dienstanweisung? 46. Erfolgen stichprobenweise Überprüfungen, ob die Mitarbeiter/innen die festgelegten Sicherheitsrichtlinien, z.B. Sperren des Rechners bei Verlassen des Arbeitsplatzes, einhalten?	Dienstanweisungen, Mitarbeitersensibilisierung, Regelungen von Verantwortlichkeiten, Berechtigungsverwaltung

		47. Ist die Einarbeitung/Einweisung neuer Mitarbeiter/innen formell geregelt? 48. Müssen neue Mitarbeiter/innen eine Verpflichtungserklärung unterzeichnen? 49. Werden Mitarbeiter/innen vor der Nutzung neuer Software entsprechend geschult? 50. Erfolgt zu den IT-Sicherheitsmaßnahmen eine Schulung der Mitarbeiter/innen? 51. Gibt es ein geregeltes Verfahren, wenn ein Mitarbeiter ausscheidet? 52. Erfolgen ausreichend Schulungen für das IT-Personal? 53. Gibt es verbindliche, von den Mitarbeitern einzufordernde Regelungen für Schulungen? 54. Müssen die IT-Mitarbeiter eine Vertraulichkeitsvereinbarung unterzeichnen?	
5	Virenschutz	55. Ist ein formelles Virenschutzkonzept vorhanden? 56. Ist das Computer- Virenschutzkonzept allen Betroffenen bekannt?	Virenschutzmaßnahmen ganzheitlich gesehen

		57. Ist eine ständige Aktualisierung der Virenschutzsoftware sichergestellt? 58. Wird ein zentrales Virenschutz-Management genutzt? 59. Werden geprüfte Dateien und erkannte/vermutete Virusinfektionen dokumentiert? 60. Sind Verhaltensregeln beim Auftreten eines Computer-Virus beschrieben und bekanntgemacht? 61. Sind Meldeketten beim Auftreten von Virusinfektionen beschrieben?	
6	Datensicherung	62. Dürfen Mitarbeiter/innen Daten lokal speichern? 63. Falls ja, gibt es eine formelle Verpflichtung der Mitarbeiter/innen diese Daten regelmäßig zu sichern? 64. Wie sieht das Gesamtkonzept für die Datensicherung aus (z.B. Bandsicherung, Backup-to-Disc, Kombinationen aus verschiedenen etc.)) 65. Wie werden die Backup Datenträger aufbewahrt, z.B. Safe, Schließfach etc.? 66. Besteht ein formelles Datensicherungskonzept?	Backupkonzept, Auslagerung, Regelungen / Zugriffe

		67. Werden regelmäßige Tests der Wiederherstellbarkeit von Datensicherungen durchgeführt? 68. In welchem Turnus werden Datensicherungen durchgeführt? 69. Wird bei der Datensicherung eine entsprechende Dokumentation hierüber angefertigt? Es genügt wenn dies automatisch über die Software erfolgt.	

5. Weiterführende Literatur

- BSI Grundschutz Kompendium 2022