Glossar

Begriffe im Kontext der Informationssicherheit

Berlin, 04.09.2024

Glossar

Nachfolgend werden die wichtigsten Begriffe rund um das Thema Informationssicherheit erklärt. Weiterführende Informationen gibt es auf der Website des Bundesamtes für Sicherheit in der Informationstechnologie (BSI) und im IT-Grundschutzkompendium des BSI.

Begriff	Definition
Anonymität	Anonymität bedeutet, dass kein Rückschluss auf den Urheber oder die Urheberin von Informationen erfolgen kann.
Anwendung/Applikation	Anwendung oder Applikation ist ein Oberbegriff für Lösungsansätze mithilfe eines Softwaresystems.
Authentizität	„Mit dem Begriff Authentizität wird die Eigenschaft bezeichnet, die gewährleistet, dass eine Kommunikationsstelle tatsächlich diejenige ist, [die] sie vorgibt zu sein. Bei authentischen Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden. Der Begriff wird nicht nur verwendet, wenn die Identität von Personen geprüft wird, sondern auch bei IT-Komponenten oder Anwendungen.“[1]
Basis-Absicherung	In der Vorgehensweise der Basis-Absicherung wird die Erfüllung der Basis-Anforderungen aus dem IT-Grundschutz überprüft. „Die Basis-Absicherung ermöglicht es, als Einstieg in den IT-Grundschutz zunächst eine breite, grundlegende Erst-Absicherung über alle Geschäftsprozesse bzw. Fachverfahren einer Institution vorzunehmen.“
Basis-Anforderung	Die Basis-Anforderungen dienen einem vereinfachten Einstieg in das Informationssicherheitsmanagement. Dabei handelt es sich um die grundlegende Erstabsicherung der Geschäftsprozesse und Ressourcen. In der Vorgehensweise der Basis-Absicherung wird somit lediglich die Erfüllung der Basis-Anforderungen überprüft.
Bausteine	„Das IT-Grundschutz-Kompendium enthält für unterschiedliche Vorgehensweisen, Komponenten und IT-Systeme Erläuterungen zur Gefährdungslage, Sicherheitsanforderungen und weiterführende Informationen, die jeweils in einem Baustein zusammengefasst sind. Das IT-Grundschutz-Kompendium ist aufgrund der Baustein-Struktur modular aufgebaut und legt einen Fokus auf die Darstellung der wesentlichen Sicherheitsanforderungen in den Bausteinen. Die grundlegende Struktur des IT-Grundschutz-Kompendiums unterteilt die Bausteine in prozess- und systemorientierte Bausteine, zudem sind sie nach Themen in ein Schichtenmodell einsortiert.“
BSI – Anforderungen für erhöhten Schutzbedarf	Unter die Anforderungen für erhöhten Schutzbedarf fällt der Schutz herausragender, besonders gefährdeter Geschäftsprozesse und Ressourcen. Eine individuelle Risikoanalyse nach dem IT-Grundschutz wird durchgeführt und besondere Schutzanforderungen werden daraus abgeleitet.

[1] Sofern keine anderen Quellen genannt werden, stammen alle wörtlichen Zitate in den Definitionen aus dem BSI-Grundschutzkompendium, Edition 2023: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4, zuletzt abgerufen am 28.08.2024.

Begriff	Definition
Business Continuity Management	„Business Continuity Management (BCM) bezeichnet alle organisatorischen, technischen und personellen Maßnahmen, die zur Fortführung des Kerngeschäfts einer Behörde oder eines Unternehmens nach Eintritt eines Notfalls bzw. eines Sicherheitsvorfalls dienen. Weiterhin unterstützt BCM die sukzessive Fortführung der Geschäftsprozesse bei länger anhaltenden Ausfällen oder Störungen.“
Cyber-Raum / Cyberspace	„Der Cyberraum (oder: Cyberspace) ist die Kurzbezeichnung für die global miteinander verbundene digitale Informations- und Kommunikations-Infrastruktur, deren bedeutendster Teil das von nahezu allen Menschen genutzte Internet ist.“[2]
Cyber-Sicherheit	„Cyber-Sicherheit befasst sich mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnik. Das Aktionsfeld der Informationssicherheit wird dabei auf den gesamten Cyber-Raum ausgeweitet. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein. Häufig wird bei der Betrachtung von Cyber-Sicherheit auch ein spezieller Fokus auf Angriffe aus dem Cyber-Raum gelegt.“
Datenschutz	„Datenschutz soll einzelne Personen davor schützen, dass diese durch den Umgang mit ihren personenbezogenen Daten in ihren Persönlichkeitsrechten beeinträchtigt werden. Mit Datenschutz wird daher der Schutz personenbezogener Daten vor etwaigem Missbrauch durch Dritte bezeichnet (nicht zu verwechseln mit Datensicherheit).“
Datenschutz-Management	„Mit Datenschutz-Management werden die Prozesse bezeichnet, die notwendig sind, um die Umsetzung der gesetzlichen Anforderungen des Datenschutzes bei der Planung, Einrichtung, dem Betrieb und nach Außerbetriebnahme von Verfahren zur Informationsverarbeitung sicherzustellen.“
Datensicherheit	„Mit Datensicherheit wird der Schutz von Daten hinsichtlich gegebener Anforderungen an deren Vertraulichkeit, Verfügbarkeit und Integrität bezeichnet. Ein modernerer Begriff dafür ist ‚Informationssicherheit‘.“
Gefahr	„‚Gefahr‘ wird oft als übergeordneter Begriff gesehen, wohingegen unter ‚Gefährdung‘ eine genauer beschriebene Gefahr (räumlich und zeitlich nach Art, Größe und Richtung bestimmt) verstanden wird. Die Gefahr ist beispielsweise ein Datenverlust. Datenverlust kann unter anderem durch eine defekte Festplatte oder Personen entstehen, der die Festplatte stehlen. Die Gefährdungen sind dann ‚defekter Datenträger‘ und ‚Diebstahl von Datenträgern‘. Diese Unterscheidung wird aber in der Literatur nicht durchgängig gemacht und ist eher von akademischer Bedeutung, sodass es sinnvoll ist, ‚Gefahr‘ und ‚Gefährdung‘ als gleichbedeutend aufzufassen.“
Gefährdung	„Eine Gefährdung ist eine Bedrohung, die konkret über eine Schwachstelle auf ein Objekt einwirkt. Eine Bedrohung wird somit erst durch eine vorhandene Schwachstelle zur Gefährdung für ein Objekt. Sind beispielsweise Schadprogramme eine Bedrohung oder eine Gefährdung für Personen, die im Internet surfen? Nach der oben gegebenen Definition lässt sich feststellen, dass alle Anwendenden prinzipiell durch Schadprogramme im Internet bedroht sind. Die Person, die eine mit Schadprogrammen infizierte Datei herunterlädt, wird von dem Schadprogramm gefährdet, wenn das IT-System anfällig für diesen Typ des Schadprogramms ist. Für Anwendende mit einem wirksamen Virenschutz, einer Konfiguration, die das Funktionieren des Schadprogramms verhindert, oder einem Betriebssystem, das den Code

[2] Siehe hier: https://www.bpb.de/shop/zeitschriften/izpb/209667/cyber-bedrohungen-aus-dem-netz/, zuletzt abgerufen am 27.08.2024.

Begriff	Definition
	des Schadprogramms nicht ausführen kann, bedeutet das geladene Schadprogramm hingegen keine Gefährdung.“
Geschäftsprozess	„Ein Geschäftsprozess ist eine Menge logisch verknüpfter Einzeltätigkeiten (Aufgaben, Arbeitsabläufe), die ausgeführt werden, um ein bestimmtes geschäftliches oder betriebliches Ziel zu erreichen.“
Informationssicherheit	„Informationssicherheit hat den Schutz von Informationen als Ziel. Dabei können Informationen sowohl auf Papier, in IT-Systemen oder auch in Köpfen gespeichert sein. Die Schutzziele oder auch Grundwerte der Informationssicherheit sind Vertraulichkeit, Integrität und Verfügbarkeit. Viele Anwendende ziehen in ihre Betrachtungen weitere Grundwerte mit ein.“
Informationssicherheitsbeauftragte:r (ISB)	„Der oder die Informationssicherheitsbeauftragte (kurz ISB oder seltener IS-Beauftragte) ist für die operative Erfüllung der Aufgabe „Informationssicherheit“ zuständig. Andere Bezeichnungen sind CISO (Chief Information Security Officer) oder Informationssicherheitsmanager oder -managerin (ISM). Die Rolle des oder der ISB sollte von einer Person mit eigener Fachkompetenz zur Informationssicherheit in einer Stabsstelle eines Unternehmens oder einer Behörde wahrgenommen werden.“
Informationssicherheitskonzept	„Mit welchen Maßnahmen die in der Leitlinie zur Informationssicherheit vorgegebenen Ziele und Strategien verfolgt werden sollen, wird in einem [Informations-]Sicherheitskonzept beschrieben. Ein solches Sicherheitskonzept hat immer einen festgelegten Geltungsbereich. Dieser wird in der IT-Grundschutz-Methodik als Informationsverbund bezeichnet.“[3]
Informationssicherheits-Management (ISM)	„Die Planungs-, Lenkungs- und Kontrollaufgabe, die erforderlich ist, um einen durchdachten und wirksamen Prozess zur Herstellung von Informationssicherheit aufzubauen und kontinuierlich umzusetzen, wird als Informationssicherheitsmanagement bezeichnet. Dabei handelt es sich um einen kontinuierlichen Prozess, dessen Strategien und Konzepte ständig auf ihre Leistungsfähigkeit und Wirksamkeit zu überprüfen und bei Bedarf fortzuschreiben sind.“
Informationsverbund	„Unter einem Informationsverbund ist die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Objekten zu verstehen, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen. Ein Informationsverbund kann dabei als Ausprägung die gesamte Institution oder auch einzelne Bereiche, die durch organisatorische Strukturen (z. B. Abteilungen) oder gemeinsame Geschäftsprozesse bzw. Anwendungen (z. B. Personalinformationssystem) gegliedert sind, umfassen.“
Infrastruktur	„Beim IT-Grundschutz werden unter Infrastruktur die für die Informationsverarbeitung und die IT genutzten Gebäude, Räume, Energieversorgung, Klimatisierung und die Verkabelung verstanden. Die IT-Systeme und Netzkoppelelemente gehören nicht dazu.“
Integrität	Integrität bezeichnet eines der drei zentralen Schutzziele in der Informationssicherheit. Die anderen beiden Schutzziele sind Vertraulichkeit und Verfügbarkeit. „Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf

[3] Siehe hier: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_2_Sicherheitsmanagement/Lektion_2_08/Lektion_2_08_node.html, zuletzt abgerufen am 27.08.2024.

Begriff	Definition
	‚Daten' angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind. In der Informationstechnik wird er in der Regel aber weiter gefasst und auf ‚Informationen' angewendet. Der Begriff ‚Information' wird dabei für ‚Daten' verwendet, denen je nach Zusammenhang bestimmte Attribute wie z. B. Autorenschaft oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zur verfassenden Person verfälscht oder Zeitangaben zur Erstellung manipuliert wurden."
IT-Grundschutz-Check	„Der Begriff bezeichnet im IT-Grundschutz die Überprüfung, ob die nach IT-Grundschutz empfohlenen Anforderungen in einer Institution bereits erfüllt sind und welche grundlegenden Sicherheitsanforderungen noch fehlen (früher: Basis-Sicherheitscheck)."
IT-Grundschutz-Kompendium	„Die Bausteine des IT-Grundschutzes sind im IT-Grundschutz-Kompendium zusammengefasst. Es stellt den Nachfolger der bis zur 15. Ergänzungslieferung verfügbaren IT-Grundschutz-Kataloge dar."
IT-Sicherheit	Die IT-Sicherheit beschreibt den Schutz der IT-Infrastruktur, zum Beispiel Server, Netzwerke, Endgeräte, Betriebssysteme und Anwendungen.
IT-System	„IT-Systeme sind technische Anlagen, die der Informationsverarbeitung dienen und eine abgeschlossene Funktionseinheit bilden. Typische IT-Systeme sind Server, Clients, Mobiltelefone, Smartphones, Tablets, IoT-Komponenten, Router, Switches und Firewalls."
Kern-Absicherung	„Im Fokus der Kern-Absicherung stehen zunächst die besonders gefährdeten Geschäftsprozesse und Assets."
Komponente	„Eine Komponente ist in der Softwarearchitektur eine eigenständig einsetzbare Einheit mit Schnittstellen nach außen, die mit anderen Komponenten verbunden werden kann. Sie ist sowohl fachlich als auch technisch unabhängig und besitzt eine gewisse Größe (im Sinne eines wirtschaftlichen Wertes). Als Komponenten werden im IT-Grundschutz technische Zielobjekte (siehe dort) oder Teile von Zielobjekten bezeichnet."
Leitlinie zur Informationssicherheit	Siehe **Sicherheitsleitlinie**
Modellierung	„Bei den Vorgehensweisen nach IT-Grundschutz wird bei der Modellierung der betrachtete Informationsverbund eines Unternehmens oder einer Behörde mit Hilfe der Bausteine aus dem IT-Grundschutz-Kompendium nachgebildet. Hierzu enthalten die Bausteine des IT-Grundschutz-Kompendiums im Kapitel „Abgrenzung und Modellierung" einen Hinweis, auf welche Zielobjekte er anzuwenden ist und welche Voraussetzungen dabei gegebenenfalls zu beachten sind."
Netzplan	„Ein Netzplan ist eine graphische Übersicht über die Komponenten eines Netzes und ihrer Verbindungen."
Risikoanalyse	„Als Risikoanalyse wird der komplette Prozess bezeichnet, um Risiken zu beurteilen (identifizieren, einschätzen und bewerten) sowie zu behandeln. Risikoanalyse bezeichnet nach den einschlägigen ISO-Normen ISO 31000 und ISO 27005 nur einen Schritt im Rahmen der Risikobeurteilung, die aus den folgenden Schritten besteht: — Identifikation von Risiken (Risk Identification) — Analyse von Risiken (Risk Analysis) — Evaluation oder Bewertung von Risiken (Risk Evaluation)

Begriff	Definition
	Im deutschen Sprachgebrauch hat sich allerdings der Begriff Risikoanalyse für den kompletten Prozess der Risikobeurteilung und Risikobehandlung etabliert. Daher wird auch in den Dokumenten zum IT-Grundschutz weiter der Begriff Risikoanalyse für den umfassenden Prozess benutzt.“
Risikomanagement	„Als Risikomanagement werden alle Aktivitäten mit Bezug auf die strategische und operative Behandlung von Risiken bezeichnet, also alle Tätigkeiten, um Risiken für eine Institution zu identifizieren, zu steuern und zu kontrollieren. Das strategische Risikomanagement beschreibt die wesentlichen Rahmenbedingungen, wie die Behandlung von Risiken innerhalb einer Institution, die Kultur zum Umgang mit Risiken und die Methodik ausgestaltet sind. Diese Grundsätze für die Behandlung von Risiken innerhalb eines ISMS müssen mit den Rahmenbedingungen des organisationsweiten Risikomanagements übereinstimmen bzw. aufeinander abgestimmt sein. Die Rahmenbedingungen des operativen Risikomanagements umfassen den Regelprozess aus — Identifikation von Risiken, — Einschätzung und Bewertung von Risiken, — Behandlung von Risiken, — Überwachung von Risiken und — Risikokommunikation.“
Schutzbedarf	„Der Schutzbedarf beschreibt, welcher Schutz für die Geschäftsprozesse, die dabei verarbeiteten Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist.“
Schutzbedarfsanalyse/Schutzbedarfsfeststellung	„Bei der Schutzbedarfsfeststellung wird der Schutzbedarf der Geschäftsprozesse, der verarbeiteten Informationen, der IT-Systeme, Räume und Kommunikationsverbindungen bestimmt. Hierzu werden für jede Anwendung und die verarbeiteten Informationen die zu erwartenden Schäden betrachtet, die bei einer Beeinträchtigung der Grundwerte der Informationssicherheit (Vertraulichkeit, Integrität oder Verfügbarkeit) entstehen können. Wichtig ist es dabei auch, die möglichen Folgeschäden realistisch einzuschätzen. Bewährt hat sich eine Einteilung in die drei Schutzbedarfskategorien ‚normal‘, ‚hoch‘ und ‚sehr hoch‘.“
Sicherheitsanforderung	„Als Sicherheitsanforderung werden Anforderungen für den organisatorischen, personellen, infrastrukturellen und technischen Bereich bezeichnet, deren Erfüllung zur Erhöhung der Informationssicherheit notwendig ist bzw. dazu beiträgt. Eine Sicherheitsanforderung beschreibt also, was getan werden muss, um ein bestimmtes Niveau bezüglich der Informationssicherheit zu erreichen.“
Sicherheitskonzept	„Ein Sicherheitskonzept dient zur Umsetzung der Sicherheitsstrategie und beschreibt die geplante Vorgehensweise, um die gesetzten Sicherheitsziele einer Institution zu erreichen. Das Sicherheitskonzept ist das zentrale Dokument im Sicherheitsprozess eines Unternehmens bzw. einer Behörde. Jede konkrete Sicherheitsmaßnahme muss sich letztlich darauf zurückführen lassen.“
Sicherheitsleitlinie	„Die Leitlinie zur Informationssicherheit (Sicherheitsleitlinie) ist ein wichtiges Grundsatzdokument der Leitung zu dem Stellenwert, den verbindlichen Prinzipien und dem anzustrebenden Niveau der Informationssicherheit in einer Institution.

Begriff	Definition
	Für die betroffenen Mitarbeiter verständlich, wird auf wenigen Seiten beschrieben, welche Sicherheitsziele angestrebt und in welchem organisatorischen Rahmen diese umgesetzt werden sollen.“[4]
Standard-Absicherung	„Die Standard-Absicherung entspricht im Wesentlichen der klassischen IT-Grundschutz-Vorgehensweise des BSI-Standards 100-2. Mit der Standard-Absicherung kann der oder die ISB die Assets und Prozesse einer Institution sowohl umfassend als auch in der Tiefe absichern.“
Standards	„Die BSI-Standards sind ein elementarer Bestandteil der IT-Grundschutz-Methodik. Sie enthalten Empfehlungen zu Methoden, Prozessen und Verfahren sowie Vorgehensweisen und Maßnahmen zu unterschiedlichen Aspekten der Informationssicherheit. Anwender aus Behörden und Unternehmen sowie Hersteller oder Dienstleister können mit den BSI-Standards ihre Geschäftsprozesse und Daten sicherer gestalten.“[5]
Strukturanalyse	„In einer Strukturanalyse werden die erforderlichen Informationen über den ausgewählten Informationsverbund, die Geschäftsprozesse, Anwendungen, IT-Systeme, Netze, Räume, Gebäude und Verbindungen erfasst und so aufbereitet, dass sie die weiteren Schritte gemäß IT-Grundschutz unterstützen.“
Verfügbarkeit	„Verfügbarkeit bezeichnet eines der drei zentralen Schutzziele in der Informationssicherheit. Die anderen beiden Schutzziele sind Integrität und Vertraulichkeit. […] Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendenden stets wie vorgesehen genutzt werden können.“
Vertraulichkeit	„Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.“
Zielobjekt	„Zielobjekte sind Teile des Informationsverbunds, denen im Rahmen der Modellierung ein oder mehrere Bausteine aus dem IT-Grundschutz-Kompendium zugeordnet werden können. Zielobjekte können dabei physische Objekte sein, z. B. IT-Systeme. Häufig sind Zielobjekte jedoch logische Objekte, wie beispielsweise Organisationseinheiten, Anwendungen oder der gesamte Informationsverbund.“

[4] Siehe hier: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_2_Sicherheitsmanagement/Lektion_2_07/Lektion_2_07_node.html, zuletzt abgerufen am 27.08.2024.

[5] Siehe hier: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/bsi-standards_node.html, zuletzt abgerufen am 27.08.2024.