IT-Grundschutz

aus SecuPedia, der Plattform für Sicherheits-Informationen

Durch Vernetzung, Nutzung des Internets vom Arbeitsplatz und eine Client/Server Architektur sind die Gefährdungen der Informationstechnik sehr komplex geworden. Verschiedene internationale Standards ermöglichen Verantwortlichen die Risikominimierung für den Betrieb von Informationstechnik. Auf nationaler Ebene hat sich bei Behörden und größeren Unternehmen der vom BSI entwickelte IT-Grundschutz etabliert. Bei internationalen Unternehmen wird dagegen eher die ISO 27001 angewandt. Für KMU bzw. kleinere Kommunen wird die VdS 3473 (neu VdS 10000) bzw. ISIS 12 (https://www.it-sicherheit-bayern.de/produkte-dienstleistungen/isis12.html) zur Vermeidung organisatorischer oder finanzieller Überforderungen empfohlen, die aber lt. BSI nur eine Vorstufe zum IT-Grundschutz darstellen.

Inhaltsverzeichnis

Ausgangslage

IT-Grundschutz ist ein pauschaliertes Vorgehen zur Minimierung der Gefährdungslage bei IT-Anwendungen bei einem normalen (früher niedrig bis mittel) Schutzbedarf. Ausgangspunkt des IT-Grundschutzes ist die Annahme, dass bei IT-Anwendungen mit normalem Schutzbedarf eine individuelle Sicherheits-Ist-Analyse und eine darauf abgestimmte Maßnahmenauswahl (Sicherheitskonzept) nicht in einem angemessenen Kosten-

Nutzen-Verhältnis zu erstellen sind. Aus diesem Grunde wurde ein Katalog mit Standardmaßnahmen aus den Bereichen Organisation, Personalwesen, Gebäude, Hardware, Software, Netze - das Grundschutz-Kompendium (früher Grundschutz-Kataloge/Grundschutzhandbuch) - definiert, um diese in pauschalierter Form im Sinne einer Mindestanforderung an ein IT-Sicherheitskonzept anzuwenden.

Die Dokumente zum IT-Grundschutz werden durch das BSI erstellt und regelmäßig an den technologischen Fortschritt angepasst. Sie bestehen im Wesentlichen aus zwei Teilen: Grundlagen des IT-Grundschutzes sowie Gefährdungen und Umsetzungshinweise (früher Maßnahmen). Im ersten Teil werden die Grundlagen für die Erstellung eines IT-Sicherheitskonzepts erläutert und Hinweise für ein geeignetes Sicherheitsmanagement gegeben (BSI-Standards). Im zweiten Teil (IT-Grundschutz-Kompendium/früher Grundschutz-Kataloge bzw. Grundschutzhandbuch) werden die Gefährdungen ausführlich beschrieben und anhand von Beispielen erläutert. Anschließend wird ein Katalog mit geeigneten Umsetzungshinweisen (früher Maßnahmen) aufgelistet. Die Edition 2019 des IT-Grundschutz-Kompendiums ist am 04. Februar 2019 erschienen und umfasst insgesamt 94 IT-Grundschutz-Bausteine.[1] Seit 1. Februar 2020 ist die 3. Edition 2020 mit 96 Bausteinen zertifizierungsrelevant. Sie löst die Edition 2019 ab, die laut BSI "für aktuelle Zertifizierungsprozesse noch bis zum 30. September 2020 gültig" ist.[2]

Reform

Im Februar 2014 teilte das BSI mit, dass eine Reform des IT-Grundschutzes geplant sei[3] und lud zu einem Workshop auf die CeBIT 2014 ein, um die Wünsche und Bedürfnis der Anwender des Standards kennenzulernen und in die Reform einzubeziehen.

Auf dem 14. Deutschen IT-Sicherheitskongress (19.-21.5.2015) berichtete der Abteilungsleiter "Cyber-Sicherheit" des BSI, Dr. Hartmut Isselhorst, dass im Jahr 2016 die ersten neuen Komponenten des reformierten IT-Grundschutzes online zur Diskussion gestellt werden sollen[4]. Die Ergebnisse wurden plangemäß auf der it-sa 2017 präsentiert[5]. Inhaltlich wurden die BSI-Standards 100-1, 100-2 und 100-3 zu den neuen Standards 200-1, 200-2 und 200-3 unter Beibehaltung der Grundausrichtung weiterentwickelt. Weiterhin wurden die früheren IT-Grundschutz-Kataloge auf das neue IT-Grundschutz-Kompendium mit besseren Strukturierung und Verschlankung umgestellt.

Im Einzelnen:

- Im Gegensatz zum alten BSI-Standard 100-2 kann der Anwender nach dem neuen BSI-Standard 200-2 zwischen 3 Vorgehensweisen zur Einführung eines Informationssicherheitsmanagementsystems (ISMS) wählen (Basis-Absicherung, Kern-Absicherung, Standard-Absicherung).
- Die alte Schichtsystematik (Schicht 1 - Übergreifende Aspekte, Schicht 2 Infrastruktur, Schicht 3 - IT-Systeme, Schicht 4 - Netze, Schicht 5 - Anwendungen) wurde durch die neue Systematik aus einer prozessorientierten Bausteinschicht (mit ISMS, ORP für Organisation und Planung, CON für Konzepte, OPS für Betrieb und DER für Detektion und Reaktion) und einer systemorientierten Bausteinschicht (mit INF für Infrastruktur, NET für Netze und Kommunikation, SYS für IT-Systeme, APP für Anwendungen und IND für industrielle IT) ersetzt.
- Der bisherige Basis-Sicherheitscheck wurde in IT-Grundschutz-Check umbenannt.
- Die Sicherheitsanforderungen im neuen Grundschutzkompendium haben nur noch Umsetzungshinweise (statt der bisher verbindlichen Umsetzungsmaßnahmen in der Grundschutz-Katalogen) und unterteilen sich in Basis-, Standard- und Anforderungen für den hohen

Schutzbedarf.

Migrationstabellen (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/Migrationstabellen.html) erleichtern die Umstellung der aus den IT-Grundschutz-Katalogen überführten Bausteinen des IT-Grundschutz-Kompendiums. Auch wurden Zuordnungstabelle (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/Zuordnung_ISO_und_modernisierter_IT_Grundschutz.html) für die Arbeit mit den beiden Vorgehensweisen ISO 27001 und IT-Grundschutz bei internationalen Unternehmen entwickelt[6].

Das BSI animiert Anwender dazu, sogenannte IT-Grundschutz-Profile des modernisierten IT-Grundschutzes zu erarbeiten, die das BSI dann veröffentlicht. Ein erstes IT-Grundschutz-Profil "Basis-Absicherung für Kommunen" wurde so bereits veröffentlicht und soll Kommunalverwaltungen beim Einstieg in den systematischen Aufbau von Informationssicherheit unterstützen[7], Schutzprofile wurden ferner unter anderem für die Handwerkskammern[8] sowie für Reedereien[9] entwickelt. Diese und weitere bisher veröffentlichten IT-Grundschutz-Profile sind auf der Informationsseite des BSI zum IT-Grundschutz (https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzProfile/Profile/itgrundschutzProfile_Profile_node.html) verfügbar.

IT-Grundschutz vor der Reform

BSI-Standards

Vor der Grundschutz-Modernisierung waren 4 IT-Grundschutz-Standards des BSI verfügbar:

1. BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS)
2. BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise
3. BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz
4. BSI-Standard 100-4: Notfallmanagement (aktuell noch weiterhin gültig)

IT-Grundschutz-Kataloge

Die einzelnen Maßnahmen der Grundschutzkataloge waren an die realen IT-Einsatzkonfigurationen approximiert. Die Einsatzrandbedingungen waren dabei in den Grundschutzkatalogen beschrieben und mussten ebenfalls berücksichtigt werden. Das Prinzip des Grundschutzes funktionierte nach dem "Baukasten"-Prinzip, wonach für jede (Standard-)IT-Konfiguration ein Maßnahmenbündel zur Erhöhung der Sicherheit dieser Konfiguration beschrieben war.

Umfeld des IT-Grundschutzes

Das BSI hat ein regelrechtes Umfeldsystem für den IT-Grundschutz geschaffen. Für IT-Verbünde und Rechenzentren besteht die Möglichkeit, sich auf Basis von IT-Grundschutz zertifizieren zu lassen. Die Prüfung, ob die hierfür festgelegten Anforderungen erfüllt werden, führt ein vom BSI lizenzierter Auditor durch. Zum Erwerb des Status als Auditor bietet das BSI Lehrgänge mit anschließender Prüfung an. Auch organisiert das BSI die jährlichen Auditorentreffen. Für den praktischen IT-Betrieb nach IT-Grundschutz kann ein von der Bundesakademie für öffentliche Verwaltung (BAköV) (im Zusammenwirken mit dem BSI) offerierter Lehrgang "IT-Sicherheitsbeauftragter der Öffentlichen Verwaltung" ebenfalls mit anschließender Prüfung und Zertifikatserteilung absolviert werden. "IT-Grundschutz-Berater" können sich direkt vom BSI schulen und zertifizieren lassen[10]

Ergänzt wird die Zertifizierung durch die IS-Revision. Diese können bereits am Anfang des Sicherheitsprozesses durchgeführt werden.

Auf Grund der umfassenden Behandlung bietet sich die IT-Grundschutz-Vorgehensweise für größere Unternehmen/Verwaltungen zur Standardisierung an (in der Bundesverwaltung und allen Bundesländern ist der IT-Grundschutz bereits IT-Sicherheits-Standard über die Leitlinie Informationssicherheit in der öffentlichen Verwaltung).

Für kleinere Unternehmen hat das BSI einen "Leitfaden zur Basis-Absicherung" entwickelt und bietet ein IT-Grundschutz-Testat nach Basis-Absicherung an[11]. Wie schon beschrieben, gibt es nach dem neuen BSI-Standard 200-2 neben der Standard-Absicherung noch die Vorstufen Basis-Absicherung (grundlegende Erstabsicherung, geeignet als Einstieg für KMU) und Kernabsicherung (Schutz besonders gefährdeter Geschäftsprozesse und Ressourcen). Zwischenzeitlich wurde jedoch auch eine etwas besser systematisierte und klarer strukturierte ISO-Norm (ISO 27003) hierfür entwickelt.

Andere Länder

In der Schweiz wurde am 27. August 2018 ein "IKT Minimalstandard" vorgestellt, der sich insbesondere an die Betreiber von kritischen Infrastrukturen in der Schweiz richtet, aber wie der deutsche IT-Grundschutz für jedes Unternehmen anwendbar ist[12].

Einzelnachweis

1. SecuPedia Aktuell: Zweite Edition des IT-Grundschutz-Kompendiums ist erschienen (https://www.secupedia.info/aktuelles/zweite-edition-des-it-grundschutz-kompendiums-ist-erschienen-12753)
2. SecuPedia Aktuell: BSI veröffentlicht IT-Grundschutz-Kompendium 2020 (https://www.secupedia.info/aktuelles/bsi-veroeffentlicht-it-grundschutz-kompendium-2020-15654)
3. SecuPedia Aktuell: Beitrag "IT-Grundschutz soll grundlegend reformiert werden" (https://www.secupedia.info/aktuelles/it-grundschutz-soll-grundlegend-reformiert-werden-1230)

4. BSI-Vortrag "IT-Grundschutz im Cyber-Raum" beim 14. Deutschen IT-Sicherheitskongress (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/ITSiKongress/14ter/Vortraege-20-05-2015/Hartmut_Isselhorst.pdf?__blob=publicationFile)
5. SecuPedia Aktuell: Der neue IT-Grundschutz: Modernisierung erfolgreich abgeschlossen (https://www.secupedia.info/aktuelles/der-neue-it-grundschutz-modernisierung-erfolgreich-abgeschlossen-9068)
6. SecuPedia Aktuell: ISO und modernisierter IT-Grundschutz: Neue Zuordnungstabelle erleichtert Arbeit mit beiden Vorgehensweisen (https://www.secupedia.info/aktuelles/iso-und-modernisierter-it-grundschutz-neue-zuordnungstabelle-erleichtert-arbeit-mit-beiden-vorgehensweisen-10520)
7. SecuPedia Aktuell: Für mehr Informationssicherheit in Kommunen: Erstes IT-Grundschutz-Profil veröffentlicht (https://www.secupedia.info/aktuelles/fuer-mehr-informationssicherheit-in-kommunen-erstes-it-grundschutz-profil-veroeffentlicht-10718)
8. SecuPedia Aktuell: IT-Grundschutz-Profil vorgestellt: Informationssicherheit im Handwerk (https://www.secupedia.info/aktuelles/it-grundschutz-profil-vorgestellt-informationssicherheit-im-handwerk-11140)
9. SecuPedia Aktuell: IT-Grundschutzprofil für Reedereien veröffentlicht (https://www.secupedia.info/aktuelles/it-grundschutzprofil-fuer-reedereien-veroeffentlicht-12468)
10. SecuPedia Aktuell: Neue Personenzertifizierung zum IT-Grundschutz-Berater (https://www.secupedia.info/aktuelles/neue-personenzertifizierung-zum-it-grundschutz-berater-13538)
11. SecuPedia Aktuell: BSI bietet IT-Grundschutz-Testat nach Basis-Absicherung (https://www.secupedia.info/aktuelles/bsi-bietet-it-grundschutz-testat-nach-basis-absicherung-13112)
12. SecuPedia Aktuell: Schweiz unterstützt Unternehmen beim Schutz vor Cyberrisiken (https://www.secupedia.info/aktuelles/schweiz-unterstuetzt-unternehmen-beim-schutz-vor-cyberrisiken-11461)

Weblinks

Das BSI betreibt eine Informationsseite zum IT-Grundschutz (https://www.bsi.bund.de/cln_174/DE/Themen/ITGrundschutz/itgrundschutz_node.html).

Bei der Verarbeitung von personenbezogenen Daten sollten immer Maßnahmen nach Vorgabe des Grundschutz-Kompendiums/der Grundschutzkataloge getroffen werden. Bestellung ist möglich über buchshop.secumedia.de (http://buchshop.secumedia.com/index.php?page=detail&match=LISA_NR2=GRUHA)

Mit verschiedenen auf dem Markt erhältlichen Softwaretools können die Maßnahmen rechnergestützt abgearbeitet und komfortabel aktualisiert werden. Eine Liste ist beim BSI einzusehen.

Siehe übergeordnete Stichworte

- IT-Notfallmanagement
- IT-Sicherheitsstrategien
- IT-Sicherheitszertifizierung

Siehe auch

- Common Criteria / ISO15408
- IS-Revision
- ISO 27001-Zertifikat auf der Basis von IT-Grundschutz
- ISO/IEC 27001 (früher BS 7799)
- IT-Sicherheits-Policy
- IT-Sicherheitsarchitektur
- IT-Sicherheitsdomäne
- IT-Sicherheitsmanagement-Pyramide
- IT-Sicherheitsprozess
- ITSEC
- ITSEM
- Plattformübergreifende Sicherheit
- Re-Zertifizierung (IT)
- Schutzprofil (IT)
- Schwachstellenbewertung (IT)
- Sicherheitsmanagement
- Sicherheitssoftware
- Sicherheitsvorgaben (IT)
- Vulnerability Assessment (Schwachstellenanalyse)

Abgerufen von „https://www.secupedia.info/w/index.php?title=IT-Grundschutz&oldid=24972“

Service-Links

Kategorien: IT-Sicherheit | IT-Sicherheitsstandardisierung

Diese Seite wurde zuletzt am 4. Februar 2020 um 15:55 Uhr von Doris Porwitzki geändert. Basierend auf der Arbeit von Oliver Wege, Peter Hohl, Ralf Schulze, Lutz Gollan, Admin, Markus Albert und Walter Ernestus.

Der Inhalt ist verfügbar unter der Lizenz Creative Commons Namensnennung-Weitergabe unter gleichen Bedingungen 3.0 Deutschland, sofern nicht anders angegeben.