Der Bundesbeauftragte für die Unterlagen
des Staatssicherheitsdienstes der ehemaligen
Deutschen Demokratischen Republik

Datum

23.05.2019

IT-Sicherheitsleitlinie (IT-SLL) des BStU

1. Vorwort / Mitgeltende Dokumente

Der Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (BStU) arbeitet auf der Grundlage des Stasiunterlagengesetzes (StUG), orientiert sich hinsichtlich der Informationssicherheit an den Vorgaben des Bundesamtes für die Sicherheit in der Informationstechnik (BSI), den Vorgaben des Ressorts der Bundesbeauftragten für Kultur und Medien (BKM), dem Umsetzungsplan Bund (UP Bund; verabschiedet am 01. September 2017 durch das Bundeskabinett und in Kraft gesetzt als Sicherheitsleitlinie für die gesamte

Bundesverwaltung).

Mitgeltende, interne Vorschriften sind die Dienstanweisung zur Nutzung und zur Sicherheit der Dienstanweisung zur Nutzung und zur Sicherheit der Informationstechnik beim BStU (DA IT) und weitere Grundsatzdokumente mit Bezug zur Informationssicherheit. Ausgangsbasis für alle getroffenen Entscheidungen und festgelegten Maßnahmen im Kontext der Informationssicherheit ist dabei grundsätzlich der Schutzbedarf der verarbeiteten Daten und Informationen.

2. Zweck

Die Informationssicherheitsleitlinie (IT-SLL) bildet die Grundlage für das Handeln des Informationssicherheitsmanagements (ISM) in der Verantwortung der Behördenleitung (BHL).

Zweck und Ziel dieses Handelns ist die Herstellung, der Erhalt und die stetige Verbesserung des erforderlichen Sicherheitsniveaus auf der Basis des Schutzbedarfs der Daten und Informationen beim BStU. Damit einher geht das zielgerichtete Erkennen von Risiken und deren Minimierung, Verlagerung und Beseitigung.

Zu diesem Zweck stellt das ISM unter der Leitung der BHL die erforderliche Aufbauorganisation, die Ablauforganisation (Prozesse) bereit und stellt geeignetes Personal und Haushaltsmittel im erforderlichen Umfang zur Verfügung.

Das ISM setzt Regelwerke in Kraft, die geeignet sind, Planung, Umsetzung und Überprüfung von Sicherheitsinvestitionen und -Maßnahmen im Geltungsbereich präventiv und perspektivisch zu gewährleisten.

Das ISM nimmt proaktiv unter Leitung der BHL seine gesetzliche Verantwortung für Informationssicherheit wahr und sorgt dafür, dass mit Hilfe eines strukturierten Sicherheitsprozesses und einer durchgängigen IT-Sicherheitskoordinierung die Sicherheitsziele des BStU erreicht werden.

3. Geltungsbereich

Die IT SLL trifft mit ihren Festlegungen generelle, allgemeingültige Aussagen zum IT Sicherheitsniveau und zur IT Sicherheitsstrategie für die gesamte Behörde des Bundesbeauftragten.

Die IT-SLL gilt verbindlich für alle Beschäftigten des BStU an allen Standorten.

Sie gilt auch für externe Beratung und Dienstleistung bei der Erledigung von Aufgaben im Auftrag des BStU und muss ihnen in geeigneter Weise zur Kenntnis und zur Beachtung gegeben werden.

4. Stellenwert der Informationssicherheit

Modernes Verwaltungshandeln erfordert zunehmend den breiten Einsatz aktueller, vernetzter Informationstechnik und übergreifender Kommunikation mit diversen internen und externen Stellen.

Diesem Erfordernis stellt sich der BStU im Sinne dieser Leitlinie mit dem Ziel, die Aufgaben, die der Gesetzgeber mit dem StUG für den BStU gefasst hat, effizient und effektiv zu erledigen. Insbesondere vor dem Hintergrund der fortschreitenden Digitalisierung der Verwaltung und der dauerhaft angespannten Gefährdungslage gewinnt die Gewährleistung der Informationssicherheit stetig an Bedeutung.

Die Kernprozesse des BStU befassen sich gem. des gesetzlichen Auftrages mit der geschichtlichen Aufarbeitung der Hinterlassenschaft des Ministeriums für Staatssicherheit der ehemaligen Deutschen Demokratischen Republik (DDR).

Es werden insgesamt Aufgaben der Forschung und der politischen Bildung, der Erschließung der Akten und der weiteren, überlieferten Materialien über Menschen und ihre Schicksale wahrgenommen. Es werden private Akteneinsichtsanträge, Anträge von Forschung und Medien sowie Ersuchen öffentlicher und nicht öffentlicher Stellen bearbeitet.

Die einzelnen Geschäftsprozesse unterliegen einem stetigen Wandel bzgl. der Anforderungen unter paralleler Anpassung der technischen Möglichkeiten. Die Digitalisierungsoffensive des Bundes gewinnt für den BStU und die Erledigung seiner Kernprozesse zunehmend an Bedeutung.

5. Bezug der Informationssicherheit zu den Zielen und Aufgaben

5.1 Sicherheitsziele

Informationssicherheit i. S. d. Leitlinie umfasst in Summe übergreifend alle organisatorischen, personellen und technischen Maßnahmen, die geeignet sind, das angestrebte Sicherheitsniveau zu erreichen und stetig zu verbessern.

Für den BStU geben die anhand der Grundwerte der Informationssicherheit (Vertraulichkeit, Verfügbarkeit und Integrität) ermittelten Schutzbedarfe der Daten und Informationen die Sicherheitsziele vor.

Die Feststellung des Schutzbedarfes erfolgt anhand einer durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) festgelegten Methodik. Hierbei sind im Einzelfall die jeweils mitgeltenden, rechtlichen Bestimmungen zu berücksichtigen.

Die Schutzbedarfsfeststellung dient dem Zweck der Sicherstellung, dass je nach dem ermittelten Schutzzweck und Schutzbedarf angemessene und dem Stand der Technik entsprechende Sicherheitsmaßnahmen ergriffen und regelmäßig revisioniert werden.

5.2 Globale Schutzziele als Ausgangsbasis

Folgende globale Schutzziele sind allgemein beim BStU maßgeblich:

Umsetzung der Aufgaben gem. StUG und Umsetzung der Informationssicherheit in Verantwortung der BHL

Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.

Verfügbarkeit von Dienstleistungen und Netzverbünden.

Funktionierende IT Systeme und IT-Anwendungen sind gegeben, wenn diese wie vorgesehen verlässlich genutzt werden können.

Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und Informationen und die korrekte Funktionsweise der Systeme, auf denen sie gehalten, transportiert und gespeichert werden. Insbesondere sind hier die Kommunikationswege und die als Mindeststandard auf den Kommunikationswegen geforderten Verschlüsselungstechnologien von besonderer Bedeutung.

Ergänzend ist vor dem Hintergrund der fortschreitenden Digitalisierung der Verwaltung der Anspruch nach Authentizität, d. h. der eineindeutigen Zuordnung der Daten und Informationen, wesentlich.

5.3 Schutzziele des BStU

Beispielhaft werden hier einige der Sicherheitsfestlegungen beim BStU aufgeführt. Die Aufzählung ist nicht abschließend. Die konkreten Einzelmaßnahmen sind den mitgeltenden Unterlagen zu entnehmen.

In den unterschiedlichen Lebenszyklusphasen von Verfahren, Fachanwendungen, IT-Systemen ist den veränderten Schutzzielen angemessen und risikobewusst Rechnung zu tragen. Die Phasen umfassen die Planung/Konzeption, Beschaffung, den Test und die Einführung, den Betrieb und die Aussonderung.

Sofern Programme und Anwendungen Sicherheitsmechanismen wie Passwortschutz und Verschlüsselung bieten, sind diese Mechanismen zu aktivieren.

Voreingestellte oder leere Passwörter sind umgehend zu ersetzen bzw. zu ändern. Wo dies nicht möglich ist, muss ggf. über einen Anbieter- oder Produktwechsel ent-schieden werden.

Passwörter, die für administrative Zwecke benötigt werden, sind an zentraler Stelle zu hinterlegen. Die Herausgabe an Berechtigte und Vertretungen erfolgt nur gegen Unterschrift.

Beim BStU gilt für die PC-Nutzung ein kaskadiertes Schutzstufenkonzept. Die Schutzstufe für die PC-Nutzung richtet sich nach der konkreten Arbeitsaufgabe und die damit verbundene Rechte- und Rollenvergabe nach Art und Umfang der benötigten Daten und Informationen am jeweiligen Arbeitsplatz.

Mobile Geräte werden als besonders sicherheitskritisch angesehen und werden daher mit geeigneten, zusätzlichen Maßnahmen vor dem Zugriff durch unbefugte Dritte geschützt.

Die Nutzung des Internets im Netzverbund erfolgt ausschließlich abgesichert durch eine Sicherheitssoftware, basierend auf dem vom BSI entwickelten Remote Control-led Browser System (ReCoBS). Ergänzt wird die Festlegung durch den zusätzlichen Einsatz eines Kategorienfilters mit unterschiedlichen Nutzungsrechten.

Der BStU orientiert sich dabei grundsätzlich an nationalen Standards, speziell den Mindeststandards des BSI. Er fordert und fördert vorrangig den Einsatz zertifizierter, deutscher Produkte und zieht für eine erforderliche Leistungserbringung im Kontext der Informationssicherheit ggf. externen Sachverstand hinzu.

Nicht mehr benötigte Datenträger und IT sind gemäß dem Stand der Technik und gem. ihres Schutzbedarfs fachgerecht zu entsorgen.

Die/der IT-SiBe initiiert und wirkt bei der Erstellung eines Notfallvorsorgekonzeptes mit. Dieses Konzept umfasst die Absicherung der Kernprozesse des BStU, definiert konkret die Situationen Störung, Krise, Katastrophe und legt in Abwägung aller Maßnahmen die maximalen Ausfallzeiten für diese Prozesse fest.

Es werden Kontroll- und Prüfaufgaben vom IT-Sicherheitsteam wahrgenommen und es sind Revisionen durchzuführen.

6. Sicherheitsstrategie und Aufbauorganisation

Die IT-Sicherheitspolitik und –kultur des BStU verfolgt strategisch die durch die Be-hördenleitung vorgegebenen IT-Sicherheitsziele unter den gegebenen Rahmenbedingungen.

Die vorliegende IT-SLL gibt den Rahmen für das Management der Informationssicherheit bei dem BStU vor.

6.1 IT-Sicherheitsmanagement (ISM)

Die Behördenleitung und die Abteilungsleitungen des BStU übernehmen die Rolle desIT-Sicherheitsmanagement (Informationssicherheit), IT-Sicherheitsverantwortlichkeiten (Rollen und Prozesse), Grundsätze. Das IT-Sicherheitsmanagement stellt die Umsetzung der IT-Sicherheitspolitik und die Erreichung der Sicherheitsziele des BStU sicher.

6.2 IT-Sicherheitsbeauftragte/r (IT-SiBe)

Die/der IT-SiBe wird von der BHL berufen. Die/der IT-SiBe handelt im Auftrag der BHL und ist erste Ansprechperson für die BHL zu allen Sicherheitsfragen beim BStU. Sie/ er koordiniert die interne Kommunikation in Sicherheitsfragen, hält den Kontakt zum Ressort BKM und ist erste Ansprechperson für das BSI.

Die/der IT-SiBe berichtet in regelmäßigen Abständen zum Status der IT-Sicherheit an das Sicherheitsmanagement und hat direktes Vortragsrecht bei der BHL.

Der/dem IT-SiBe werden zur Erfüllung ihrer/seiner Aufgaben die erforderlichen Ressourcen bereitgestellt und geeignete Qualifizierungsmaßnahmen ermöglicht.

6.3 IT-Sicherheitsteam

Das IT-Sicherheitsteam des BStU besteht neben der/dem IT-SiBe aus den jeweiligen IT-Sicherheitsbeauftragten der Fachabteilungen (IT-SiBe F), die als Ansprechperson für die Informationssicherheit in diesen Abteilungen zuständig sind. Insbesondere die/ der IT-SiBe F der Fachabteilung ZV, die/ der mit 90 % ihrer/ seiner regelmäßigen Arbeitszeit mit der Wahrnehmung der Aufgaben betraut ist, ist erste/r Ansprechpartner für Sicherheitsfragen an das Fachreferat IT/TK. Sie/ er ist gleichzeitig Fachadministrator/in der Sicherheitssoftware, in der das behördliche Sicherheitskonzept gehalten wird. Die IT SiBe F der Abteilungen AR, AU, BF und Regionales sind im Dialog mit den IT Koordinatoren erste Ansprechpersonen für die jeweilige Abteilung und wenden sich bei übergreifenden Fragen an die/den behördlichen IT-SiBe.

7. Umsetzung der Informationssicherheitsleitlinie

Zur Erreichung und Aufrechterhaltung des angestrebten Sicherheitsniveaus werden im erforderlichen Maße Personal- und Finanzmittel bereitgestellt. Diese werden in Abstimmung mit

den Verfahrensverantwortlichen/ Fachbereichen und der/ dem jeweiligen IT-SiBe eingeplant.

Dort, wo Grundschutz ausreichend ist, werden die Maßnahmen nach dem Grundsatz der Verhältnismäßigkeit und der Praktikabilität ausgewählt und umgesetzt.

Werden im Rahmen der Schutzbedarfsfeststellung gem. der weiterführenden BSI Methodik Risiken erkannt, so werden diese behandelt, verlagert, beseitigt und / oder auf der Basis von Entscheidungen des ISM getragen.

Stehen mehrere alternative Maßnahmen zur Erreichung eines Sicherheitsziels zur Verfügung, so wird diejenige ausgewählt, die hinsichtlich der Investitionen und Be-triebskosten die wirtschaftlichste und perspektivisch die sicherste ist.

Dokumentierte Restrisiken werden von der Behördenleitung auf Basis einer Sicherheitsmanagemententscheidung getragen.

Die Beschäftigten werden regelmäßig und bedarfsgerecht für die Belange der IT Sicherheit im Rahmen von Schulungen und Workshops sensibilisiert.

Jede/r Einzelne muss in die Lage versetzt sein, durch verantwortungs- und sicherheitsbewusstes Handeln sowohl materiellen als auch ideellen Schaden, respektive Imageverluste, vom BStU abzuwenden.

Die umzusetzenden Sicherheitsmaßnahmen werden für die Beschäftigten transparent und verständlich formuliert. Die Beschäftigten werden über konkrete Sicherheitsmaßnahmen nach der Maßgabe: „Informationen im angemessenen Umfang“ informiert.

Alle Beschäftigten des BStU sind darüber hinaus verpflichtet, sich über den Inhalt der IT-SLL eigenständig und regelmäßig zu informieren und sich mit deren Festlegungen vertraut zu machen.

Beschäftigte sind bei der Erstellung, Nutzung und Verwaltung von Daten und Informationen dazu verpflichtet, die IT-SLL und alle darüber hinaus geltenden Vorschriften einzuhalten.

8. Verpflichtung zur kontinuierlichen Verbesserung

Informationssicherheit ist kein unveränderlicher Zustand, sondern hängt von vielen internen und externen Rahmenbedingungen und Einflüssen ab. Beispielhaft zu nennen sind neue Bedrohungen, neue und geänderte Gesetzesgrundlagen und / oder auch der Entwicklung und der Einsatz neuer technischer Lösungen.

Aus diesem Grund trägt das ISM in der Verantwortung der Behördenleitung dafür Sorge, dass die Sicherheitsstrategie kontinuierlich fortentwickelt wird.

Die Behördenleitung bezieht dafür die/den IT-SiBe und das Sicherheitsteam rechtzeitig in die strategischen Planungen ein und holt sich dafür, je nach Art und Umfang der Aufgabe, externen Sachverstand ein.

Festgelegte Sicherheitsmaßnahmen sind regelmäßig auf Akzeptanz und Wirksamkeit zu kontrollieren und die Überprüfung ist nachweisbar zu dokumentieren.

Die Beschäftigten sind angehalten, mögliche Verbesserungen oder Schwachstellen/aufgetretene Risiken in Zusammenhang mit der Erhaltung und Verbesserung des Sicherheitsniveaus an die entsprechenden Stellen weiterzugeben.

9. Schlussbestimmung und Inkraftsetzung

Zur Verbesserung der Informationssicherheit finden regelmäßige Überprüfungen statt, ob der Sicherheitsprozess und die eingeführten Managementstrukturen funktionieren und den mit dieser IT-SLL aufgestellten Qualitätsansprüchen genügen.

Allen Beschäftigten des BStU muss deutlich sein, dass missbräuchliche, gegen die Festlegungen der IT-SLL gerichtete Handlungen dienst- und/oder strafrechtliche Konsequenzen nach sich ziehen können.

Die IT-Sicherheitsleitlinie (IT-SLL) tritt mit Veröffentlichung in Kraft, gleichzeitig soll die IT-Sicherheitsleitlinie vom 09.06.2009 außer Kraft gesetzt werden.

Berlin, den

gez. I. V. Deicke
Der Bundesbeauftragte