Bundesamt
für Sicherheit in der
Informationstechnik

Umsetzungshinweise zum Baustein CON.11.1 Geheimschutz VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)

1. Einleitung

Der staatliche Geheimschutz umfasst alle Maßnahmen zur Geheimhaltung von Informationen, die durch eine staatliche Stelle oder auf deren Veranlassung als Verschlusssachen (VS) eingestuft worden sind. VS sind im öffentlichen Interesse, insbesondere zum Schutz des Wohles des Bundes oder eines Landes, geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse, unabhängig von ihrer Darstellungsform.

Der staatliche Geheimschutz wird durch Vorschriften des Bundes- und des Landesrechts geregelt. Rechtliche Grundlage für den staatlichen Geheimschutz des Bundes ist das Sicherheitsüberprüfungsgesetz (SÜG). Für den materiellen Geheimschutz des Bundes ist die Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung – VSA) maßgeblich. Diese richtet sich an Bundesbehörden oder bundesunmittelbare öffentlich-rechtliche Einrichtungen (Dienststellen), die mit Verschlusssachen arbeiten. Beim Einsatz von Informationstechnik zur Handhabung von VS (VS-IT) sind die Anforderungen der VSA zu beachten. Voraussetzung für den Einsatz von VS-IT ist die Einhaltung der Standards zur Informationssicherheit des BSI in der jeweils geltenden Fassung.

2. Maßnahmen

Im Folgenden sind spezifische Maßnahmen für die Anforderungen des Bausteins *CON.11.1 Geheimschutz VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)* aufgeführt.

Alle Maßnahmen (gekennzeichnet mit M) sind aufsteigend nummeriert und korrespondieren mit den entsprechenden Anforderungen (gekennzeichnet mit A).

2.1. Maßnahmen zum Baustein CON.11.1 Geheimschutz VS-NUR FÜR DEN DIENSTGEBRAUCH

CON.11.1.M1 Einhaltung der Grundsätze zur VS-Verarbeitung mit IT nach § 3, 4 und 6 und Nr. 1 Anlage V zur VSA (B)

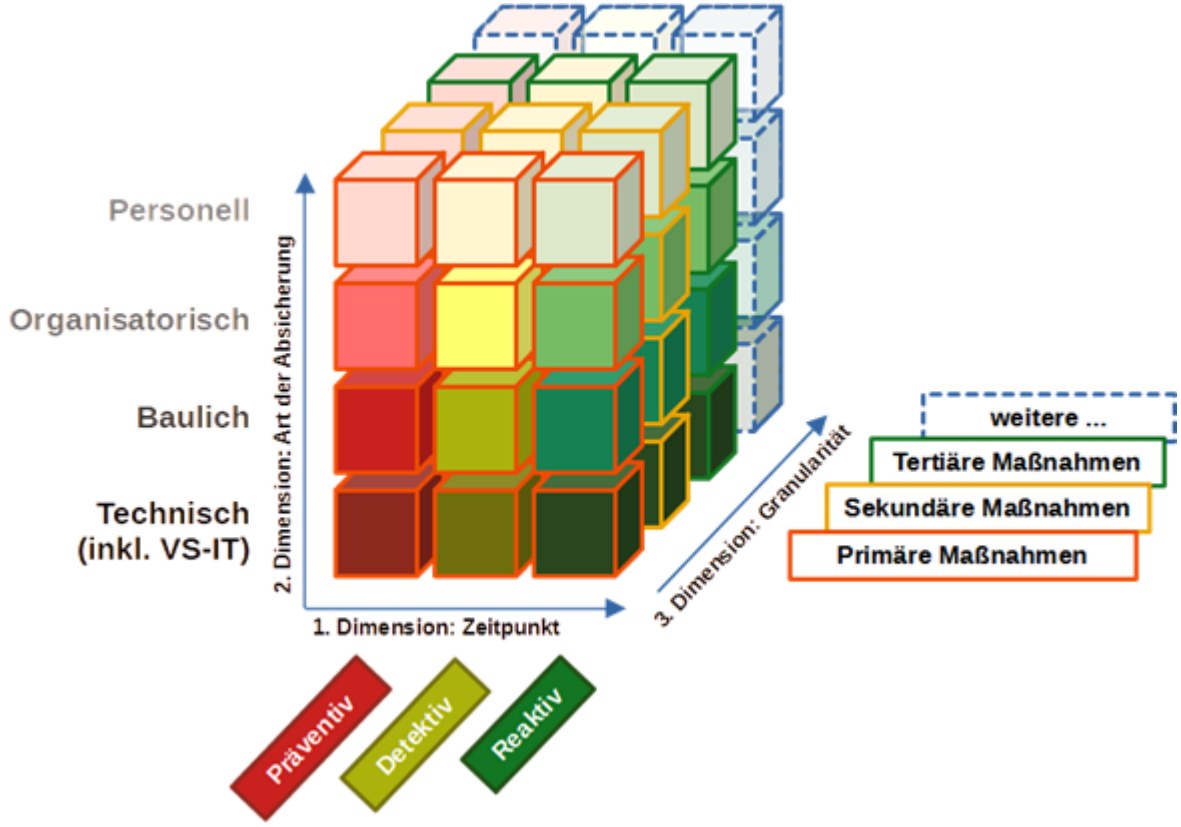
In der zugehörigen Anforderung werden die zwei zentralen Grundsätze des Geheimschutzes behandelt. Ziel ist es, dass die Grundsätze "Kenntnis nur, wenn nötig" und „Mehrschichtige Sicherheit“ frühzeitig in den Planungen von VS-IT berücksichtigt werden.

Kenntnis nur, wenn nötig

Der Grundsatz "Kenntnis nur, wenn nötig" bedeutet, dass eine Person erst Kenntnis von einer VS erlangen darf, wenn hierfür ein dienstliches Interesse vorliegt. Alleine die Verwendung von freigegebener VS-IT berechtigt nicht grundsätzlich zur Kenntnisnahme aller gespeicherten VS. Auch reicht der Verweis auf ausschließlich personelle Maßnahmen nicht aus. Diese müssen durch materielle (organisatorische, bauliche, technische) Maßnahmen ergänzt werden. Die VS-IT spezifischen Maßnahmen sind in den nachfolgenden Anforderungen zu behandeln. Bei der Auswahl der zu ergreifenden Maßnahmen ist es notwendig, den Geltungsbereich der VS-IT zu berücksichtigen. Dabei müssen auch weitere Informationsverbünde betrachtet werden, zu denen Schnittstellen existieren. Wird beispielsweise VS-IT von Dienstleistenden zur Verarbeitung von VS mitgenutzt, dann ist der Gesamtverbund übergreifend zu betrachten. Eine ausschließliche Betrachtung der VS-IT, die im eigenen Zuständigkeitsbereich liegt, reicht NICHT aus.

Mehrschichtige Sicherheit

Bei der Wahl der Maßnahmen ist es wichtig, dass die verschiedenen Maßnahmen sinnvoll ineinandergreifen. Das Ziel der "Mehrschichtigen Sicherheit" ist es, die Risiken für einen erfolgreichen Angriff auf die VS bzw. ggf. VS-IT so weit wie möglich zu reduzieren und im Falle eines erfolgreichen Angriffs die Auswirkungen zu minimieren. Zur Umsetzung ist es daher wichtig zu dokumentieren, wie die gewählten Maßnahmen zur Umsetzung der Geheimschutzanforderungen zusammenspielen.



Die Abbildung 1 veranschaulicht das Zusammenspiel anhand eines Würfels, der aus vielen kleinen Elementen besteht. Die Abbildung ist folgendermaßen aufgebaut:

- **Dimension: Zeitpunkt** - Die Elemente werden anhand des Zeitpunkts, an dem die Maßnahmen im Falle eines Angriffs greifen (präventiv, detektiv und reaktiv), unterschieden.
- **Dimension: Art der Absicherung** - Die Elemente werden nach der Art der Absicherung (technisch (inklusive VS-IT), baulich, organisatorisch, personell) unterschieden.
- **Dimension: Granularität** - Die Elemente werden nach ihrer Granularität, in welchem Bereich eine Maßnahme greift (primär, sekundär, tertiär, ...), unterschieden. Hierunter ist zu verstehen, dass beispielsweise im IT-Bereich eine primäre Maßnahme den Schutz für die gesamte VS-IT gewährleistet, während eine tertiäre Maßnahme den Schutz eines einzelnen Clients gewährleistet. In einem anderen Beispiel wird eine Papier-VS durch die Bewachung der Liegenschaft (primäre Maßnahme), das Einrichten eines Sicherheitsbereiches (sekundäre Maßnahme) und die Verwahrung in einem verschlossenen Behältnis (tertiäre Maßnahme) geschützt.

Es ist hierbei zu beachten, dass sich das dargestellte Würfelmodell je nach gewähltem Absicherungsszenario aus verschiedenen Elementen mit unterschiedlicher Gewichtungen zusammensetzen kann. Jedes Element besteht aus drei Dimensionen. Die gewählten Maßnahmen lassen sich einem der Elemente zuordnen. Im Idealzustand gibt es zu jedem Element des Würfels dazugehörige Maßnahmen, die sinnvoll ineinandergreifen. Da der Idealzustand aufgrund äußerer Rahmenbedingungen in der Regel nicht in Gänze abgebildet werden kann, müssen Defizite durch die stärkere Gewichtung anderer Elemente ausgeglichen werden.

Lässt sich beispielsweise in der Dimension der Granularität der Perimeter aufgrund äußerer Umstände nicht hinreichend absichern, dann werden die Maßnahmen der nachfolgenden Granularitätsstufen (sekundär, tertiär, ...) wichtiger. Im umgekehrten Fall, wenn sich beispielsweise aus Kostengründen aufwändige Maßnahmen der sekundären und nachfolgenden Stufe nicht ausreichend umsetzen lassen, muss der Perimeter besonders gut abgesichert werden (beispielsweise durch organisatorische, bauliche und technische Maßnahmen). Diese zwei Szenarien beschreiben beispielhafte Situationen, in denen

innerhalb einer Stufe Abstriche gemacht werden müssen und sich die Schwerpunkte der Absicherung auf die anderen Granularitätsstufen verlagern. Diese Betrachtungsweise lässt sich analog auf die anderen beiden Dimensionen übertragen.

Zusammenfassung

Zur Umsetzung dieser Anforderung ist es daher erforderlich darzulegen, wie die Grundsätze „Kenntnis nur, wenn nötig“ und "Mehrschichtige Sicherheit" konkret umgesetzt werden. Dabei ist NICHT gemeint, dass in der Umsetzungsbeschreibung alle Maßnahmen, die insgesamt vorgesehen wurden, detailliert niedergeschrieben werden. Stattdessen ist der Fokus auf die Darstellung der äußeren Rahmenbedingungen und der daraus abgeleiteten übergreifenden, grundlegenden Absicherungsstrategie der VS und ihrer verarbeitenden VS-IT zu legen. Der übergreifende Fokus soll darstellen, wie die einzelnen Maßnahmen innerhalb der drei Dimensionen miteinander verzahnt sind und wie damit den vorgegebenen Rahmenbedingungen begegnet wird. Ferner soll diese Vorgehensweise sicherstellen, dass ein sinnvolles sowie ergänzendes Ineinandergreifen der Maßnahmen erfolgt und keine Dimension vergessen wird.

Ein pauschaler Verweis auf einzelne singulär betrachtete Anforderungen ist nicht zielführend. Im Rahmen einer zusammenhängenden Gesamtdarstellung sind konkrete Verweise (Dokument, Kapitel, ggf. Seite) auf weiterführende Dokumente möglich, soweit eine Einordnung in die Gesamtzusammenhänge erfolgt.

CON.11.1.M2 Erstellung und Fortschreibung der VS-IT-Dokumentation nach § 12 und Nr. 2.2 Anlage II zur VSA (B)

Damit die Geheimschutzbeauftragten einen Überblick über vorhandene VS-IT und deren Zustand haben, ist es wichtig, dass eine VS-IT-Dokumentation gepflegt wird. Hierfür sind die Geheimschutzbeauftragten oder besonders beauftragte Mitarbeitende zuständig. Für die Bereitstellung der benötigten Informationen und Unterlagen werden die Geheimschutzbeauftragten durch die Verantwortlichen für den Betrieb der jeweiligen VS-IT und die Informationssicherheitsbeauftragten unterstützt.

Die Umsetzung dieser Anforderung sollte nicht durch das Beifügen der VS-IT-Dokumentation erfolgen. Die VS-IT-Dokumentation sollte nur bei Bedarf vor Ort eingesehen werden. Stattdessen empfiehlt sich ein Interview mit den Geheimschutzbeauftragten und Verweise auf relevante Kapitel der VS-IT-Dokumentation. Es sollte dargelegt werden, dass eine VS-IT-Dokumentation geführt und gepflegt wird und in welchen Abständen diese auf Aktualität, Vollständigkeit und Erforderlichkeit überprüft wird.

Allgemeine Fragen zur VS-IT-Dokumentation

Es sollten die folgenden allgemeinen Fragen beantwortet werden:

Wer?

- Wer ist verantwortlich für die Erstellung und Pflege der VS-IT-Dokumentation?

Wo?

- Wo wird die VS-IT-Dokumentation aufbewahrt?

Wann? Wie oft?

- Wie häufig wird die VS-IT-Dokumentation auf Aktualität und Vollständigkeit überprüft?
- Wann wurde sie das letzte Mal überprüft bzw. aktualisiert?
- Wird die VS-IT-Dokumentation nach geheimschutzrelevanten Änderungen aktualisiert?

Wie?

- In welcher Form liegt die VS-IT-Dokumentation vor (z. B. digital, in Papierform, hybrid)?
- Wie werden die Geheimschutzbeauftragten in den Änderungsprozess miteinbezogen?

- Wie unterstützen die Informationssicherheitsbeauftragten die Erstellung und Fortschreibung der VS-IT-Dokumentation? Alternativ: Wie werden die Informationssicherheitsbeauftragten einbezogen?
- Anhand welcher Kriterien entscheiden die Geheimschutzbeauftragten, ob eine geheimschutzrelevante Änderung vorliegt?

Was?

- Existiert eine VS-IT Dokumentation?

Fragen zur betrachteten VS-IT.

Zusätzlich sollten für die betrachtete VS-IT folgende Fragen behandelt werden:

Wer?

- Wer ist zuständig für die VS-IT und Ansprechpartner für die Geheimschutzbeauftragten?

Wann?

- Wann wurden die Geheimschutzbeauftragten miteinbezogen?
- Wurde in der Vergangenheit die wirksame Umsetzung der Geheimschutzanforderungen überprüft und die Überprüfung dokumentiert?
    - Falls ja, wann war das?

Was?

- Sind die Nachweise zur Einhaltung der BSI-Standards zur Informationssicherheit in der VS-IT-Dokumentation enthalten?
- Verfügt die betrachtete VS-IT über eine Freigabe?
    - Falls ja, erfolgte diese mit Auflagen?
    - Falls ja, ist diese Freigabe dokumentiert?
- Wurde die Freigabe der VS-IT in der Vergangenheit widerrufen?
    - Falls ja, was war der Grund für den Widerruf?
- Sind die Zulassungsnachweise und Einsatzerlaubnisse der eingesetzten IT-Sicherheitsprodukte in die VS-IT-Dokumentation aufgenommen worden?

Sind die Komponenten, die in der VS-IT IT-Sicherheitsfunktionen erfüllen, dokumentiert?

CON.11.1.M3 Einsatz von IT-Sicherheitsprodukten nach §§ 51, 52 VSA (B)

Hinweise zur Umsetzung der Anforderung CON.11.1.A3 *Einsatz von IT-Sicherheitsprodukten nach §§ 51, 52 VSA (B)* sind folgenden Dokumenten zu entnehmen:

- Katalog der Produktklassen und –typen (VS-Produktkatalog), gem. § 52, Abs. 2 VSA [VS-Produktkatalog]
- Aktuelle Liste zugelassener IT-Sicherheitsprodukte und –komponenten (BSI Schrift 7164), gem. § 52, Abs. 2 VSA [BSI Schrift 7164]
- Mitwirkungspflichten in Zulassungsverfahren (Technische Leitlinie BSI TL - IT 01), gem. § 52, Abs. 1 VSA [BSI TL – IT 01]

CON.11.1.M4 Beschaffung von VS-IT nach § 49 VSA (B)

VS sind während ihres gesamten Lebenszyklus zu schützen. Das gilt gleichermaßen für VS-IT, die ab dem Zeitpunkt, zu dem feststeht, dass sie zur VS-Verarbeitung eingesetzt werden soll, kontinuierlich geschützt werden muss. Ein kritischer Zeitpunkt ist die Beschaffung, da bereits hier zum Schutz der VS Anforderungen an die VS-IT festgelegt und an den Auftragnehmer kommuniziert werden müssen.

Frühzeitige Einbindung

Es ist wichtig, dass die Geheimschutzbeauftragten frühzeitig in den Beschaffungsprozess eingebunden und die Anforderungen des Geheimschutzes bei der Erstellung der Leistungsbeschreibung für die Beschaffung berücksichtigt werden. Sollte der Geheimschutz erst danach berücksichtigt werden, dann besteht die Gefahr, dass Produkte beschafft werden, mit denen es nicht möglich ist, die Geheimschutzanforderungen zu erfüllen. Dies betrifft auch Beauftragungen von Firmen sowie Dienstleistende, da sich die auftraggebende Stelle Kontrollrechte vertraglich zusichern lassen muss, wenn VS im Auftrag verarbeitet oder erstellt werden (vgl. Nr. 6.6 Anlage V zur VSA).

IT-Sicherheitsprodukte

Für den Aufbau einer VS-IT ist es wichtig, dass vor der Beschaffung die Auswahl geeigneter IT-Sicherheitsprodukte erfolgt (vgl. CON.11.1.*A3 Einsatz von IT-Sicherheitsprodukten nach §§ 51, 52 VSA (B)*). Falls die BSI- Schrift 7164 für eine zulassungspflichtige Teilkomponente kein geeignetes IT-Sicherheitsprodukt aufführt, sind mit dem BSI die Zulassungsmöglichkeiten abzustimmen. In der Beschaffung muss festgelegt werden, dass der Hersteller bei der Zulassung mitwirkt, denn ansonsten kann das Zulassungsverfahren nicht erfolgreich durchlaufen werden (vgl. [BSI TL - IT 01]).

Hardware

Darüber hinaus muss bei der Beschaffung von Hardware, mit welcher VS verarbeitet werden soll oder möglicherweise werden könnte, vertraglich festgeschrieben sein, dass alle Datenträger oder sonstige Komponenten, auf denen VS gespeichert sein könnten, im Besitz der Dienststelle verbleiben. Damit soll verhindert werden, dass während einer Wartung oder Reparatur, die nicht vor Ort durchgeführt wird, Dritte Kenntnis über VS erlangen.

Zusätzlich ist bei der Beschaffung von Datenträgern darauf zu achten, ob die VS von diesen gelöscht werden können oder die Datenträger nach der Verwendung vernichtet werden müssen (siehe CON.11.*A13 Löschung elektronischer VS, Vernichtung von Datenträgern und IT-Produkten nach §§ 32, 56 und Nr. 8 Anlage V zur VSA (B)*). Ist beides nicht möglich, müssen andere Maßnahmen zum Schutz der VS ergriffen werden, bspw. Verschlüsselung der VS durch zugelassene IT-Sicherheitsprodukte.

Software

Falls Software beschafft werden soll, die keine IT-Sicherheitsfunktionen zum Schutz der VS implementiert, ist im Vorhinein zu klären, wie der Schutz der VS (beispielsweise die Speicherung (siehe CON.11.1.A9 *Speicherung elektronischer VS nach § 23 und Nr. 5 Anlage V zur VSA (B)*)) sichergestellt wird. Darüber hinaus ist zu klären, wie die VS ausgesondert bzw. an das Archiv abgegeben werden kann. Gegebenenfalls muss die Software hierfür geeignete Schnittstellen bereitstellen (siehe CON.11.1.A12 *Archivierung elektronischer VS nach §§ 30, 31 VSA (B)*).

Vorgehen

Es ist wichtig, dass dargestellt wird, wie die Geheimschutzbeauftragten in die Beschaffung eingebunden wird. Dazu besteht die Möglichkeit auf bestehende Prozesse zu verweisen und die entsprechenden Dokumente beizufügen. Dabei sollten mindestens die folgenden Fragen adressiert werden:

Wer?

- Sind die Geheimschutzbeauftragten eingebunden?

Wo?

- Kommen geheimschutzbezogene Interessen zum Tragen, die eine Ausschreibung, bspw. im Ausland, untersagen?

Wann? Wie oft?

- Wann wurden die Geheimschutzbeauftragten bezüglich der Beschaffung eingebunden?
- Wurden IT-Sicherheitsfunktionen vor der Beschaffung identifiziert und geeignete IT-Sicherheitsprodukte ausgewählt?

Wie?

- Wie sind die Geheimschutzbeauftragten in den Beschaffungsprozess eingebunden?

Was?

- Werden die Anforderungen des Geheimschutzes bei der Erstellung einer Anforderungsliste für die Beschaffung berücksichtigt?
- Wurden alle erforderlichen Vorgaben an den Auftragnehmer in die Ausschreibungsunterlagen aufgenommen, bspw. Bereiterklärung der Mitarbeitenden zur Verpflichtung und Kontrollrechte des Auftraggebers?
- Wurde der Hersteller dazu verpflichtet, bei einem Zulassungsverfahren mitzuwirken?

Zusätzlich ist für die betrachtete VS-IT anzugeben, welche Anforderungen des Geheimschutzes bei der Beschaffung wie berücksichtigt werden, welche IT-Sicherheitsprodukte beschafft werden und ob Zulassungsanträge für IT-Sicherheitsprodukte gestellt wurden, die noch keine Zulassungsaussage besitzen, aber eine oder mehrere zulassungsrelevante IT-Sicherheitsfunktionen erfüllen.

Darüber hinaus sollten je nach Art der Beschaffung die getroffenen Maßnahmen mit der sich aus der Erfüllung der folgenden Anforderungen ergebenen Maßnahmen abgeglichen werden:

- ORP.5.A2 *Beachtung der Rahmenbedingungen (B),*
- OPS.1.2.5.A9 *Auswahl und Beschaffung geeigneter Fernwartungswerkzeuge (S),*
- APP.3.1.A9 *Beschaffung von Webanwendungen und Webservices (S),*
- APP.6.A3 *Sichere Beschaffung von Software (B),*
- APP.7.A7 *Sichere Beschaffung von Individualsoftware (S),*
- SYS.1.1.A13 *Beschaffung von Servern (S),*
- SYS.2.1.A11 *Beschaffung von Clients (S),*
- SYS.3.3.A7 *Beschaffung von Mobiltelefonen (S),*
- SYS.4.3.A4 *Erstellung von Beschaffungskriterien für eingebettete Systeme (S),*
- NET.3.1.A11 *Beschaffung eines Routers oder Switches (S),*
- NET.3.2.A15 *Beschaffung einer Firewall (B),*
- NET.4.1.A13 *Beschaffung von TK-Anlagen (S).*

Die Maßnahmen sollten ineinandergreifen und sich gegenseitig sinnvoll ergänzen.

CON.11.1.M5 Verpflichtung bei Zugang zu VS nach § 4 VSA und Anlage V zur VSA (B)

Die Verpflichtung auf Anlage V der VSA ist eine Voraussetzung, damit Personen Zugang zu VS des Geheimhaltungsgrades VS-NfD erhalten können. Damit gewährleistet ist, dass alle in Frage kommenden Personen verpflichtet sind, ist es nötig, dass die Geheimschutzbeauftragten einen Prozess etabliert. Dabei sollten mindestens die folgenden Fragen beantwortet werden:

Wer?

- Wer führt die Verpflichtung durch?
- Wer ist für den Prozess der Verpflichtung zuständig?
- Wer ist dafür verantwortlich, dass die Anlage V zur VSA zugänglich gemacht wird?
- Wer muss aufgrund seiner Tätigkeit verpflichtet werden?
- Wer könnte Zugang zu VS erlangen?

Wann?

- Wann werden Personen verpflichtet?

Wie?

- Wie ist der Prozess der Verpflichtung in der Behörde gestaltet?
- Wie wird die Anlage V zur VSA den verpflichteten Personen zugänglich gemacht?
- Wie wird mit Fremdpersonal umgegangen?
- Wird eine Dokumentation über die verpflichteten Personen geführt?

Was?

- Gibt es Fälle, in denen von einer Verpflichtung von Fremdpersonal abgesehen wurde?
    - Unter welchen Bedingungen?
    - Ist dies dokumentiert?

Zur Umsetzung dieser Anforderung ist der Prozess zu dokumentieren und beizufügen.

CON.11.1.M6 Beaufsichtigung und Begleitung von Fremdpersonal für VS-IT nach §§ 3, 4 VSA (B)

Grundsätzlich ist Fremdpersonal zu verpflichten. Davon darf abgesehen werden, falls nur kurzfristig an VS-IT gearbeitet wird und ein Zugriff auf VS ausgeschlossen werden kann. Damit der Schutz von VS weiterhin gegeben ist, muss das eingesetzte Fremdpersonal begleitet und beaufsichtigt werden. Die Beaufsichtigung muss in der Lage sein, die Tätigkeiten des Personals nachvollziehen und die Auswirkungen auf die VS-IT bewerten zu können.

Vorgehen

Zur Umsetzung der Anforderung sind entsprechende Vorgaben zur Beaufsichtigung und Begleitung von Fremdpersonal zu beschreiben oder auf bestehende Dokumente zu verweisen. Falls auf andere Dokumente verwiesen wird, sind die entsprechenden Passagen beizufügen. Generell sollten unter anderem die folgenden Fragen beantwortet werden:

Wer?

- Wird nicht verpflichtetes Fremdpersonal begleitet?
- Wer begleitet das Fremdpersonal?
- Erfolgt die Beaufsichtigung durch fachkundiges Personal?
- Steht für die Beaufsichtigung ausreichend fachkundiges Personal zur Verfügung?

Wo?

- Wohin wird das nicht verpflichtete Fremdpersonal begleitetet?
- Gibt es einen (öffentlichen) Bereich, in dem das nicht verpflichtete Fremdpersonal sich alleine frei bewegen kann?
- Wo werden öffentliche Bereiche von nichtöffentlichen Bereichen (in denen das Fremdpersonal begleitet werden muss) abgegrenzt?

Wann? Wie oft?

- Wie häufig wird nicht verpflichtetes Fremdpersonal benötigt?

Wie?

- Wie wird sichergestellt, dass die Aufsichtsperson über die notwendige Fachkenntnis verfügt?
- Wie ist der Personalschlüssel zwischen den zu beaufsichtigenden und dem Aufsichtspersonal?

Was?

- Wofür wird nicht verpflichtetes Fremdpersonal eingesetzt?
- Welche Vorgaben zur Beaufsichtigung und Begleitung von Fremdpersonal für VS-IT existieren in der Dienststelle?

Bei der Umsetzung dieser Anforderung sind unter anderem die getroffenen Maßnahmen zu den IT-Grundschutz-Anforderungen ORP.1.A3 *Beaufsichtigung oder Begleitung von Fremdpersonen (B)* und ORP.2.A4 *Festlegung von Regelungen für den Einsatz von Fremdpersonal (B)* entsprechend zu berücksichtigen. Gleichzeitig ist auch die Anforderung CON.11.1.A5 *Verpflichtung bei Zugang zu VS nach § 4 VSA und Anlage V zur VSA (B)* zu berücksichtigen.

CON.11.1.M7 Kennzeichnung von elektronischen VS und Datenträgern nach §§ 20, 54 und Anlage III, V und VIII zur VSA (B)

Die Kennzeichnung von VS ist eine zentrale Vorgabe, da ansonsten ein Objekt nicht als VS erkannt werden kann und eine erforderliche Absicherung unterbleibt. Es ist daher zwingend erforderlich, dass die Kennzeichnung einer VS über die gesamte Lebenszeit und über jedes Medium hinweg gewährleistet ist. Dies bedeutet, dass nicht nur Papierdokumente gekennzeichnet sein müssen, sondern auch digitale Objekte. Das können zum Beispiel neben Textdokumenten, E-Mails auch Video-, Bild- und Audiodateien sein.

Die VSA macht Vorgaben, wie die Kennzeichnung auszusehen hat (siehe Anlage IV, V und VIII zur VSA). Komplexer als bei Papier ist dies beispielsweise bei Audio-, Bild- und Videodateien, hier hat die Kennzeichnung sinngemäß zu erfolgen. Eine Möglichkeit ist, den Geheimhaltungsgrad durchgehend in der Videodatei einzublenden. Bei einer Audiodatei könnte mündlich die VS-Einstufung genannt werden.

Dienstleistende

Hinsichtlich der Nutzung von Dienstleistenden, die (Cloud-)Plattformen für die VS-Verarbeitung bereitstellen, ist folgendes zu beachten. Sollen für die elektronische Verarbeitung von VS Dienstleistungen Dritter genutzt werden, dann müssen die Dienstleistenden gegenüber der Dienststelle darlegen, wie die Kennzeichnung in seinen IT-Systemen umgesetzt wird. Dies betrifft vor allem die Speicherung von VS im SAN oder das Erzeugen von Backups. Auch dort muss die VS entsprechend gekennzeichnet sein.

Ein weiterer Aspekt ist, dass nicht nur elektronische VS gekennzeichnet werden müssen, sondern auch IT-Produkte und Datenträger, auf denen VS unverschlüsselt oder mit einem IT-Sicherheitsprodukt ohne Zulassungsaussage verschlüsselt gespeichert sind.

Vorgehen

Zur Umsetzung dieser Anforderung ist es hilfreich, wenn die in der Dienststelle geltenden Vorgaben (Vorgaben zur Kennzeichnung, Schulungskonzept etc.) entsprechend beschrieben oder auf bestehende Dokumente verwiesen wird. Falls auf andere Dokumente verwiesen wird, sind die entsprechenden Passagen beizufügen. Generell sollten unter anderem die folgenden Fragen beantwortet werden:

Wer?

- Werden die Mitarbeitenden in der Kennzeichnung von VS geschult?
- Werden die Mitarbeitenden darin geschult, dass diese wissen, wann ein Datenträger als VS zu kennzeichnen ist?
- Wer überprüft, dass die VS ordnungsgemäß gekennzeichnet werden?

Wann? Wie oft?

- Wie oft werden Mitarbeitende in der Kennzeichnung von VS geschult?

Wie?

- Wie erfolgt die Kennzeichnung in einer ggf. selbst- oder für die VS-IT entwickelten Software?
- Ist die Kennzeichnung auch ohne das Öffnen eines Dokuments erkennbar?
- Bleibt die Kennzeichnung bei einem Datenexport/Ausdruck weiterhin gewährleistet?
- Welche Vorgaben zur Kennzeichnung von Dokumenten existieren in der Behörde? Existieren Dokumentenvorlagen, die diese Vorgaben berücksichtigen?
- Gibt es Vorgaben zur Kennzeichnung von IT-Produkten und Datenträgern, aus denen klar hervorgeht, wann und wie der Mitarbeitende diese zu kennzeichnen hat?

Was?

- In Verbindung mit CON.11.1.A9 *Speicherung elektronischer VS nach § 23 und Nr. 5 Anlage V zur VSA (B)* und CON.11.1.A15 *Handhabung von Datenträgern und IT-Produkten nach § 54 und Anlage V zur VSA (B)*: Werden die Datenträger, auf denen VS nicht entsprechend der Vorgaben der VSA verschlüsselt werden, geeignet gekennzeichnet?

Bei der Kennzeichnung von Datenträgern ist zusätzlich die Anforderung SYS.4.5.A13 *Kennzeichnung der Wechseldatenträger beim Versand (S)* zu beachten.

CON.11.1.M8 Verwaltung und Nachweis von elektronischen VS nach § 21 VSA (B)

VS des Geheimhaltungsgrads VS-NfD können unter Einhaltung des Grundsatzes „Kenntnis nur, wenn nötig“ in offenen Registraturen verwaltet werden. Dabei sind die Grundsätze ordnungsgemäßer Aktenführung einzuhalten (siehe hierzu die Registraturrichtlinien des BMI [REG-R]).

Diese Anforderung bedeutet nicht, dass die Absicherung der VS-IT auf ein "Sicherheitsniveau ohne VS" herabgesetzt werden kann. Generell ist zu beachten, dass bei VS, die mit IT verarbeitet werden, die IT gemäß der höchsten darauf verarbeiteten VS abzusichern ist. Die Anforderung ist aus der Handhabung von VS mit Papier abgeleitet, dass VS-NfD nicht zwingend in VS-Registraturen aufbewahrt werden müssen, sondern die klassische Registratur durch den Verschluss der Räumlichkeiten bzw. personelle Besetzung die materielle Absicherung gewährleistet. Ein Übertragen auf die Verarbeitung mit IT ist ohne eine entsprechende Absicherung der VS-IT nicht möglich.

Vorgehen

Zur Umsetzung dieser Anforderung ist es sinnvoll darzustellen, wie die Aktenführung von VS-NfD eingestuften Dokumenten in der Behörde erfolgt. Dabei sollten folgende Fragen beantwortet werden:

Wer?

- Werden die Mitarbeitenden im Umgang der ordnungsgemäßen Aktenführung geschult?

Wann? Wie oft?

- Wie häufig wird diese Schulung angeboten?

Wie?

- Wie wird in der Behörde die Aktenführung von VS-NfD eingestuften Dokumenten umgesetzt?

Zusätzlich kann ein Verweis auf die Umsetzung von CON.11.1.A1 *Einhaltung der Grundsätze zur VS-Verarbeitung mit IT nach § 3, 4 und 6 und Nr. 1 Anlage V zur VSA (B)* helfen, um darzulegen, dass der Grundsatz "Kenntnis nur, wenn nötig" eingehalten wird und damit die VS in offenen (elektronischen) Registraturen verwaltet werden kann.

CON.11.1.M9 Speicherung elektronischer VS nach § 23 und Nr. 5 Anlage V zur VSA (B)

Bei der Speicherung von VS ist es wichtig, sich nicht nur auf die Clients zu fokussieren. Der Schutz der VS muss auch auf Servern, im Rechenzentrum und bei der Verarbeitung durch Dienstleistende gewährleistet sein. Dies gilt auch, falls von der VS ein Backup erstellt wird.

Es gibt verschiedene Möglichkeiten, die VS zu schützen:

- Eine VS des Geheimhaltungsgrades VS-NfD kann in Papierform aufbewahrt werden, in dem diese in einem verschlossenen Behältnis oder Raum aufbewahrt wird. Auf die gleiche Weise kann eine elektronische VS geschützt werden. Der Datenträger oder der Client kann in einem verschlossenen Raum oder Behältnis aufbewahrt werden, falls ein anderer Zugriff (beispielsweise über eine Netzverbindung) während der Aufbewahrung ausgeschlossen werden kann.
- Es besteht auch die Möglichkeit, die VS mithilfe eines IT-Sicherheitsprodukts mit Zulassungsaussage zu verschlüsseln. Diese Möglichkeit eignet sich beispielsweise für zentrale Speicherorte, auf die regelmäßig für andere Zwecke zugegriffen wird.
- Eine weitere Möglichkeit ist die Verschlüsselung des gesamten Datenträgers. Hierbei wird nicht die einzelne VS verschlüsselt, sondern der Datenträger ist im ausgeschalteten Zustand durch ein IT-Sicherheitsprodukt mit Zulassungsaussage verschlüsselt. Der Nachteil ist, dass dieser Schutz nur im ausgeschalteten Zustand greift.

Vorgehen

Zur Beantwortung dieser Anforderung empfiehlt es sich, den in der Dienststelle festgelegten Prozess zur Speicherung von VS zu beschreiben oder auf entsprechende Dokumente zu verweisen und diese beizufügen. Dabei sollten unter anderem die folgenden Fragen beantwortet werden:

Wer?

- Wer benötigt Zugriff auf die gespeicherten VS?

Wo?

- Wo werden VS gespeichert, ggf. auch zwischengespeichert oder verarbeitet?
- Ist eine materielle Sicherung der VS möglich?
- Wo existieren temporäre Dateien?
- Wo liegen die Schlüssel zur Entschlüsselung von VS? Wer/welche IT-Systeme hat Zugriff auf den Schlüssel?

Wann?

- Wie oft muss auf die VS zugegriffen werden?

Wie?

- Wie erfolgt die Speicherung (Verwendung eines IT-Sicherheitsproduktes mit Zulassungsaussage, im Klartext?)
- Welche Regelungen existieren zur Speicherung von VS auf Wechseldatenträgern? Ist sichergestellt, dass bei gemeinsam genutzten Datenträgern nur solche VS gespeichert werden, für die die jeweiligen Nutzenden ein gemeinsames Need-to-Know haben?
- Welche Regelungen existieren zur Speicherung von VS auf gemeinsam genutzten Speichermedien (z. B. Netzlaufwerke)? Existiert eine geeignete Zugriffs- und Rechteverwaltung?

Was?

- Welche materiellen Maßnahmen werden ggf. ergriffen?

Falls die Speicherung der VS durch Dienstleistende erfolgt, beispielsweise durch die Nutzung bereitgestellter Dienste, dann müssen die Dienstleistenden für den Schutz der VS bei der Speicherung und beim Backup Sorge tragen. Dienstleistende haben der nutzenden Dienstelle auf Verlangen entsprechende Nachweise zur Verfügung stellen.

Falls durch das Speichern einer VS ein Datenträger selbst zur VS wird, sind die entsprechenden Anforderungen CON.11.1.A7 *Kennzeichnung von elektronischen VS und Datenträgern nach §§ 20, 54 und Anlage III, V und VIII zur VSA (B)* und CON.11.1.A15 *Handhabung von Datenträgern und IT-Produkten nach § 54 und Anlage V zur VSA (B)* einzubeziehen.

CON.11.1.M10 Elektronische Übertragung von VS nach §§ 24, 53, 55 und Nr. 6.2 Anlage V zur VSA (B)

Die VS ist auch während der Übertragung zu schützen. Diese Anforderung beleuchtet verschiedene Übertragungswege:

- innerhalb einer Liegenschaft,
- zwischen mehreren Liegenschaften,
- zwischen verschiedenen Dienststellen sowie
- an Dritte.

Die Erfüllung dieser Anforderung ist komplex, da hier das gesamte Netz, die Netzübergänge und andere Übertragungswege im Fokus stehen. Es ist darzustellen, über welche Strecken VS übertragen wird und wie dort der Schutz gewährleistet wird.

Da eine Verschlüsselung zu Leistungseinbußen führt, ist es wichtig abzuschätzen, welche Übertragungswege vertrauenswürdig und geschützt sind. Diese Betrachtung muss immer Szenario-spezifisch erfolgen. Kann ein unbefugter Zugriff ausgeschlossen werden, darf auf diesen Übertragungswegen auf eine Verschlüsselung verzichtet werden. Bei Funkverbindungen (z. B. WLAN, Bluetooth) muss immer auf eine Verschlüsselung mittels IT-Sicherheitsprodukte mit Zulassungsaussage zurückgegriffen werden.

Vorgehen

Anhand eines Netzplanes sollte dargelegt werden, auf welchen Übertragungswegen VS übertragen wird. Zusätzlich ist deutlich zu machen, ob diese Wege baulich, materiell oder auf anderem Wege (z. B. Verschlüsselung) geschützt werden. Bei der Beantwortung sollten unter anderem folgende Fragen beantwortet werden:

Wer?

- Mit welchen „Gegenstellen“ sollen VS ausgetauscht werden?
    - Innerhalb der Liegenschaft
    - Andere Liegenschaften?
    - Andere Behörden?
    - Externe Dritte?
- Sind beide Anschlusspunkte/Dienststellen für die Verarbeitung von VS freigegeben?

Wo?

- Über welche Leitungsstrecken werden VS geführt?

Wie?

- Wie sind die (Eingangs-/Ausgangs-) Schnittstellen abgesichert?
- Wie wird ein Zutritt-, Zugangs- und Zugriffsschutz auf die Übertragungseinrichtung einschließlich Kabel und Verteiler realisiert?
- In welcher Form werden die Daten übertragen?
- Werden die Daten durch ein IT-Sicherheitsprodukt mit Zulassungsaussage verschlüsselt oder im Klartext versendet?

- Welche materiellen Maßnahmen zur Leitungssicherung werden ergriffen? (Bspw. bei Steigleitungen, in Tiefgarage)
- Ist das Transportnetz für die Verarbeitung von VS freigegeben?
- Findet ein Umschlüsseln statt, weil bspw. unterschiedliche Zuständigkeiten für die Netzbereiche vorliegen? Sind diese Bereiche, in denen VS ent- und neu verschlüsselt werden, gegen unbefugten Zugang geschützt?
- Netzübergänge: Wie werden Daten übertragen (verschlüsselt/unverschlüsselt) und an welchen Stellen (Netzübergänge/Endpunkte) werden die Daten überprüft, bspw. auf Integrität oder Schadcode?

Was?

- Welche (Eingangs-/Ausgangs-) Schnittstellen existieren?
- Welche absehbaren Kommunikationsszenarien werden abgedeckt bzw. auf welche IT-Systeme soll im Rahmen außergewöhnlicher Lagen zurückgegriffen werden?
- Kann in diesen Lagen der Schutz der VS weiter gewährleistet werden?

Dienstleistende

Werden Dienstleistende für die Verarbeitung von VS eingebunden, sind entsprechende Nachweise der Dienstleistenden einzuholen. Hinsichtlich der Nutzung von Dienstleistenden, die (Cloud-)Plattformen für die VS-Verarbeitung bereitstellen, ist folgendes zu beachten:

- Da die Dienststellen keinen Einfluss auf die Absicherung der Netze der Dienstleistenden haben, ist es Aufgabe der Dienstleistenden dort für den Schutz bei der Übertragung der VS zu sorgen und dies gegenüber der Dienststelle auch nachweisen zu können.
- Könne die Dienstleistenden diesen Nachweis nicht erbringen, muss die Dienststelle sicherstellen, dass ein Zugriff auf die VS für die Dienstleistenden nicht möglich ist, bspw. durch Einsatz von IT-Sicherheitsprodukten mit Zulassungsaussage.

Bezüglich der Übertragung zu anderer VS-IT ist die Anforderung CON.11.1.A16 *Zusammenschaltung von VS-IT nach § 58 VSA (B)* zu berücksichtigen. Darüber hinaus sind die Maßnahmen so zu treffen, dass diese die Maßnahmen, die zur Umsetzung der Anforderung der nachfolgenden IT-Grundschutz-Bausteine getroffen wurden, sinnvoll erweitern und mit denen ineinandergreifen:

- CON.9 *Informationsaustausch,*
- NET.1.1 *Netzarchitektur und –design,*
- NET.2.1 *WLAN-Betrieb,*
- NET.3.1 *Router und Switches,*
- NET.3.2 *Firewall*,
- NET.3.3 *VPN* und
- INF.12 *Verkabelung*

Darüber hinaus kann es je nach Einsatzszenario sinnvoll sein, dass die gewählten Maßnahmen mit den getroffenen Maßnahmen zur Umsetzung der nachfolgenden Anforderungen sinnvoll ineinandergreifen:

- CON.7.A16 *Integritätsschutz durch Check-Summen oder digitale Signaturen (H*),
- OPS.3.2.A10 *Etablierung eines sicheren Kommunikationskanals und Festlegung der Kommunikationspartner (S),*
- SYS.4.1.A1 *Planung des Einsatzes von Druckern, Kopierern und Multifunktionsgeräten (B),*

- SYS.4.1.A11 *Einschränkung der Anbindung von Druckern, Kopierern und Multifunktionsgeräten (S),*
- SYS.4.1.A14 *Authentisierung und Autorisierung bei Druckern, Kopierern und Multifunktionsgeräten (H).*

CON.11.1.M11 Mitnahme elektronischer VS nach § 28 VSA und Nr. 7 Anlage V zur VSA (B)

Die VSA handhabt die Mitnahme von VS sehr strikt. Dies hat zur Folge, dass VS nur auf Dienstreisen und zu Dienstbesprechungen mitgenommen werden dürfen, sofern dies dienstlich notwendig ist. In Einzelfällen können die Geheimschutzbeauftragten Ausnahmeregelungen treffen. Die ausschließlich elektronische Verarbeitung von VS ist außerhalb der Dienstliegenschaft mit hierfür freigegebener VS-IT auch in der Privatwohnung zulässig.

Vorgehen

Zur Umsetzung dieser Anforderung ist es wichtig, dass die getroffenen Maßnahmen detailliert dargelegt werden. Es ist zu beschreiben, welche technischen und organisatorischen Maßnahmen dies ermöglichen bzw. unterstützen. Dabei sollten unter anderem die folgenden Fragen beantwortet werden:

Wer?

- Sind die Mitarbeitenden bezüglich der Mitnahme von VS sensibilisiert und unterrichtet worden?

Wo?

- Wohin dürfen Mitarbeitende VS mitnehmen?

Wie?

- Welche Regelungen zur Mitnahme von VS existieren in der Behörde?
    - Für Dienstreisen?
    - Für Dienstreisen ins Ausland?
    - In das Homeoffice, beim mobilen Arbeiten?

Was?

- Welche IT-Komponenten sind für die Mitnahme erlaubt?
- Wurden vom Geheimschutzbeauftragten Ausnahmeregelungen getroffen?

Zusätzlich sollten bei der Beantwortung unter anderem auf die Erkenntnisse aus den IT-Grundschutz-Checks der Bausteine CON.7 *Informationssicherheit auf* Auslandsreisen und INF.8 *Häuslicher Arbeitsplatz* und der Anforderungen SYS.4.5.A5 *Regelung zur Mitnahme von Wechseldatenträgern (S*) und INF.9.A2 *Regelungen für mobile Arbeitsplätze (B)* Bezug genommen werden. Darüber hinaus sollte das „Merkblatt für den Umgang mit mobiler Informationstechnik bei Mitnahme ins Ausland“, welches vom BSI veröffentlicht wird, beachtet werden.

CON.11.1.M12 Archivierung elektronischer VS nach §§ 30, 31 VSA (B)

Nach dem Bundesarchivgesetz werden VS des Geheimhaltungsgrades VS-NfD wie nicht eingestufte Informationen ausgesondert. Anbietung und Abgabe von VS-NfD eingestuften VS werden bereits bei den üblichen Abgabeverfahren für papiergebundene und elektronische Unterlagen berücksichtigt. Um frühzeitig die organisatorischen und technischen Anforderungen zu ermitteln und die erforderlichen Standards (gemäß § 5 Abs. 3 BArchG) festzulegen, ist mit dem Bundesarchiv Kontakt aufzunehmen. Neben einem Beratungsangebot stellt das Bundesarchiv zusätzlich Handreichungen und Merkblätter zur Aussonderung elektronischer Unterlagen auf seinen Internetseiten bereit. Die Beantwortung dieser

Anforderung sollte im Regelfall durch ein Interview des Geheimschutzbeauftragten möglich sein, in dem die folgenden Fragen beantwortet werden:

Wer?

- Ist den Mitarbeitenden bekannt, wie elektronischer VS zu archivieren sind?
- Wer ist in der Behörde verantwortlich für die Archivierung?
- Wer gestaltet den entsprechenden Prozess?

Wann?

- Nach wie vielen Jahren werden elektronische VS dem Archiv angeboten?

Wie?

- Wie ist der Prozess zur Archivierung definiert?
- Wurde der Prozess zur Archivierung mit dem Bundesarchiv abgestimmt?

Was?

- Wird bei der Beschaffung bzw. Entwicklung von Services/Software berücksichtigt, dass eine Möglichkeit zur Archivierung von VS bereitzustellen ist?
- Falls externe Dienstleistende Services zur VS-Verarbeitung bereitstellen:
    - Bieten diese Möglichkeiten zur Archivierung an?
    - Sind die behördeninternen Prozesse mit den Dienstleistenden abgestimmt?

Sollte es einen dokumentierten Prozess zur Archivierung elektronischer VS geben, kann dieser beigefügt und darauf verwiesen werden. Es kann hilfreich sein, für die Bearbeitung dieser Anforderung die Erkenntnisse aus den IT-Grundschutz-Checks des Bausteins OPS.1.2.2 *Archivierung* zu berücksichtigen.

CON.11.1.M13 Löschung elektronischer VS, Vernichtung von Datenträgern und IT-Produkten nach §§ 32, 56 und Nr. 8 Anlage V zur VSA (B)

Das Löschen und Vernichten stellt einen essentiellen Bestandteil im Lebenszyklus von VS dar.

Löschen

Gewöhnliche Löschvorgänge über die Funktionen des Betriebssystems bewirken in der Regel kein sicheres Löschen der VS, das verhindert, dass die VS wieder rekonstruiert werden können. Um VS so zu löschen, dass vom Inhalt weder Fragmente übrigbleiben, noch Fragmente wiederhergestellt werden können, bedarf es daher spezieller Verfahren. Die Löschung von VS muss mittels IT-Sicherheitsprodukten mit Zulassungsaussage erfolgen.

Beim Verschlüsseln elektronischer VS durch ein IT-Sicherheitsprodukt mit Zulassungsaussage wird Schlüsselmaterial generiert, das zum Entschlüsseln benötigt wird. Um verschlüsselte VS zu löschen, muss das Schlüsselmaterial entsprechend der Vorgaben der Einsatz- und Betriebsbedingungen (engl. SecOps) sicher gelöscht werden. Zu beachten ist, dass auch alle Sicherheitskopien der Schlüssel gelöscht werden müssen.

Wenn VS, die nicht durch ein IT-Sicherheitsprodukt mit Zulassungsaussage verschlüsselt wurden, gelöscht werden sollen, dann besteht nur die Möglichkeit, den ganzen Datenträger zu löschen. Aber auch dies ist nicht immer ohne Probleme möglich. Bei modernen Datenträgern wie SSDs werden durch einen vollständigen Löschvorgang nicht alle Bereiche des Datenträgers überschrieben. Es besteht auch nach mehreren Löschvorgängen weiterhin die Gefahr, dass Fragmente einer VS erhalten bleiben und somit auch wieder rekonstruiert werden könnten.

Zur Umsetzung dieser Anforderung sind in Bezug auf das Löschen von VS unter anderem die folgenden Fragen relevant:

Wer?

- Wer ist verantwortlich für die Löschung von VS und den zugrundeliegenden Prozess?
- Ist allen Mitarbeitenden bekannt, dass Datenträger, die nicht sicher gelöscht wurden, das Haus nicht verlassen dürfen?
    - Werden die Vorgaben zum Löschen von VS beachtet?
    - Wie wird dies sichergestellt?
- Werden die Mitarbeitenden im Umgang mit dem Löschen elektronischer VS sensibilisiert und geschult?
- Wer führt die Löschung von VS durch?

Wo?

- Wo wird die Löschung durchgeführt?
- Wo liegen VS vor und können die VS daraus gelöscht werden? (auch Drucker, Scanner, Datenträger, temporärer Speicher etc.)

Wie?

- Ist ein Prozess für das Löschen von Datenträgern, auf denen VS unverschlüsselt gespeichert wurden, vorgesehen?
- Wurden vor der geplanten Löschung der VS die VS dem Archiv angeboten?

Was?

- Ist die Löschung auch bei einem Einsatzwechsel eines Datenträgers (bei gleichbleibender Einstufung) gewährleistet?
- Werden die Vorgaben der SecOPs des zur Verschlüsselung eingesetzten IT-Sicherheitsproduktes bei der Löschung berücksichtigt?
- Die Löschung muss mittels IT-Sicherheitsprodukten mit Zulassungsaussage erfolgen. Welche Produkte kommen hierfür zum Einsatz?
- Werden beim Löschen durch ein IT-Sicherheitsprodukt mit Zulassungsaussage die entsprechenden Vorgaben der SecOPS berücksichtigt?

Vernichten

Ist das Löschen der VS nicht möglich, muss der gesamte Datenträger physisch vernichtet werden. Hierbei sind die Vorgaben der [BSI TL - M 50] einzuhalten und folgende Fragen relevant:

Wer?

- Wer ist verantwortlich für die Vernichtung von VS?
- Wer führt die Vernichtung von VS durch?
- Werden die Mitarbeitenden zur Vernichtung von VS geschult?

Wo?

- An welchen Stellen im Gebäude können welche Datenträger (Papier, HDD, SSD, Bänder etc.) vernichtet werden?
    - Nach welchem Standard vernichten die jeweiligen Geräte?
    - Erfüllen die jeweiligen Geräte die Anforderungen der BSI TL - M 50?

Wann?

- Wann kann eine Vernichtung durchgeführt werden (jederzeit, nach Absprache, an festen Terminen)?

Wie?

- Gibt es einen Prozess zur Aussonderung/Vernichtung von Datenträgern?
- Wird die Löschung bzw. Vernichtung in der Geheimschutzdokumentation dokumentiert?

Dienstleistende

Hinsichtlich der Nutzung von Dienstleistenden, die (Cloud-)Plattformen für die VS-Verarbeitung bereitstellen ist folgendes zu beachten:

- Dienstleistende haben dafür Sorge zu tragen, dass das Löschen von VS möglich ist. Die Dienststelle kann dies nicht gewährleisten, da diese keinen Zugang zu den physischen Speichermedien hat.
- Dienstleistende müssen dafür sorgen, dass auch bei der Verwendung eines SAN das Löschen von VS möglich ist. Eine Möglichkeit ist eine Verschlüsselung der VS durch ein IT-Sicherheitsprodukt mit Zulassungsaussage, bevor diese auf dem SAN gespeichert werden. Alternativ müssen alle Daten auf dem SAN durch ein IT-Sicherheitsprodukt mit Zulassungsaussage verschlüsselt werden. Wird VS unverschlüsselt im SAN gespeichert, ist es sehr schwierig die Festplatte zu identifizieren, auf der die VS im SAN-Verbund gespeichert wurde.
- Ist ein Löschen von VS im SAN nicht möglich, dann sind die Datenträger als VS zu behandeln bis die Datenträger entsprechend den Vorgaben der VSA vernichtet wurden.
- Der Umgang mit dem Löschen und Vernichten von VS sollte zwischen den Dienstleistenden und der Dienststelle abgestimmt und in entsprechenden vertraglichen Regelungen festgehalten werden.

Zur Umsetzung dieser Anforderung in Bezug auf die Nutzung von Dienstleistenden sollten unter anderem die folgenden Fragen ggf. von beauftragten Dienstleistenden beantwortet werden:

Wer?

- Welche Dienstleistenden verarbeiten die VS?
- Wer ist bei den Dienstleistenden verantwortlich für das Löschen und Vernichten von VS, die die Dienststelle bei den Dienstleistenden verarbeitet?

Wo?

- Wo lassen die Dienstleistenden Datenträger vernichten, auf denen VS der Dienststelle gespeichert sind?

Wann?

- Wie schnell setzen die Dienstleistenden einen Lösch- oder Vernichtungsauftrag der Dienststelle um?

Wie?

- Wie löschen oder vernichten die Dienstleistenden VS der Dienststelle?
- Sind die Prozesse mit der Dienststelle abgestimmt?
- Werden der Dienststelle Nachweise über die Löschung/Vernichtung vorgelegt?

Bei der Bearbeitung dieser Anforderung ist die Umsetzung des Bausteins CON.6 *Löschen und Vernichten* und die BSI TL - M 50 zu beachten. Beim Beauftragen von Dienstleistenden ist zusätzlich der Baustein OPS.2.*3 Nutzung von Outsourcing* zu berücksichtigen. Für Dienstleistende ist der Baustein OPS.3.2 *Anbieten von Outsourcing* zu berücksichtigen.

Zur Umsetzung dieser Anforderung ist es wichtig darzulegen, wie der Prozess zum Löschen und Vernichten von VS in der Behörde organisiert ist. Dazu kann entweder auf entsprechende Dokumente

verwiesen und diese beigefügt, oder der Prozess unter Zuhilfenahme der oben aufgelisteten Fragen innerhalb der Umsetzungsbeschreibung dargestellt werden.

CON.11.1.M14 Zugangs- und Zugriffsschutz nach § 3 VSA (B)

Zugang

In Anlehnung an die Definition des IT-Grundschutz-Kompendiums wird mit "Zugang" die Nutzung von VS-IT-Systemen, Teilkomponenten und Netzen bezeichnet. Zugangsberechtigungen erlauben somit einer Person, bestimmte Ressourcen wie VS-IT-Systeme oder Teilkomponenten und Netze zu nutzen.

Zugriff

Mit "Zugriff" wird die Kenntnisnahme von VS bzw. die Nutzung von Informationen oder Daten bezeichnet. Über Zugriffsberechtigungen wird geregelt, welche Personen im Rahmen ihrer Funktionen oder welche IT-Anwendungen bevollmächtigt sind VS, Informationen, Daten oder auch IT-Anwendungen, zu nutzen oder Transaktionen auszuführen.

Zutritt

Nicht betrachtet wird der "Zutritt". Darunter wird das Betreten von abgegrenzten Bereichen wie z. B. Räumen oder geschützten Arealen in einem Gelände bezeichnet. Zutrittsberechtigungen erlauben somit Personen, bestimmte Umgebungen zu betreten, also beispielsweise ein Gelände, ein Gebäude oder definierte Räume eines Gebäudes. Die VSA stellt zur Absicherung von VS des Geheimhaltungsgrades VS-NfD keine Anforderungen an den Zutrittsschutz, der über den IT-Grundschutz hinausgehen. Daher sind zur Umsetzung des Zutrittsschutzes die relevanten Bausteine der Schicht INF umzusetzen.

Bei der Betrachtung des Zugangs- und Zugriffsschutzes sind neben den Rechenzentren und Liegenschaften zwingend auch die Übertragungswege zu berücksichtigen. Dies schließt sowohl leitungsgebundene als nicht leitungsgebundene (z. B. WLAN) Übertragungswege ein.

Vorgehen

Die Absicherung sollte so gewählt werden, dass folgende Fragen dabei berücksichtigt wurden:

Wer?

- Wer benötigt Zugang zu der VS-IT und warum?
    - Nutzende
    - Administratoren
    - Externe Dienstleistende
    - weitere?
- Sind die Personen verpflichtet?
- Wer hat Zugriff auf VS und warum?
    - Nutzende
    - weitere?
    - Sind die Personen verpflichtet?
- Haben diese Personen einen berechtigten Grund für die Kenntnis über die VS?

Wo?

- Von wo aus ist ein Zugang zur VS-IT möglich?
    - Rechenzentrum
    - Übertragungswege

  - Liegenschaft
  - Homeoffice
  - unterwegs?
- Von wo kann auf die VS zugegriffen werden?
  - Rechenzentrum
  - Liegenschaft
  - Übertragungswege
  - Homeoffice
  - unterwegs?
- Wo findet eine Authentifizierung der Nutzenden statt?

Wann? Wie oft?

- Gibt es Zeiträume, in denen der Zugangs- und Zugriffsschutz nicht gewährleistet werden kann? (z.B. Abwesenheit der Admins, fehlende Überwachung der Protokollierung, längere Reaktionszeiten)
  - Wenn ja: Wann und warum?

Wie?

- Wie wird der Zugang zur VS-IT kontrolliert?
- Wie wird der Zugriff auf VS kontrolliert?
- Wie werden die Netzübergänge der VS-IT geschützt?
  - Verwendung einer PAP-Struktur mit Zulassungsaussage?
- Wie wird das Need-to-Know beim Zugriff auf VS umgesetzt?
- Können VS, auch auf Datenträgern oder in Backups, explizit dem Herausgeber der VS zugeordnet werden?

Was?

- Was für Sicherheitsmaßnahmen wurden getroffen?
  - im Rechenzentrum
  - in den Liegenschaften
  - auf den Übertragungswegen
  - im Homeoffice
  - unterwegs
  - in weiteren Situationen?
- Welche technischen Sicherheitsmaßnahmen wurden ergriffen, um einen unerlaubten Zugriff auf VS zu verhindern?
- Welche Authentisierungsmechanismen existieren und greifen diese ineinander?
- Existiert ein Rechte-Rollen-Konzept?

Für die Umsetzung des Zugangsschutzes sind Maßnahmen zu treffen, welche die in den folgenden IT-Grundschutz-Bausteinen getroffenen Maßnahmen zum Zugangsschutz sinnvoll ergänzen:

- ORP.4 *Identitäts- und Berechtigungsmanagement,*
- OPS.1.1.2 *Ordnungsgemäße IT-Administration,*

- SYS.1.1 *Allgemeiner Server,*
- SYS.1.5 *Virtualisierung,*
- SYS.1.6 *Containerisierung,*
- SYS.1.8 *Speicherlösungen,*
- NET.1.1 *Netzarchitektur und –design,*
- NET.3.1 *Router und Switches* und
- NET.3.2 *Firewall.*

Für die Umsetzung des Zugriffsschutzes sind Maßnahmen zu treffen, welche die in den folgenden IT-Grundschutz-Bausteinen getroffenen Maßnahmen zum Zugriffsschutz sinnvoll ergänzen:

- ORP.4 *Identitäts- und Berechtigungsmanagement,*
- SYS.1.1 *Allgemeiner Server,*
- SYS.1.8 *Speicherlösungen,*
- SYS.2.1 *Allgemeiner Client* und
- SYS.4.1 *Drucker, Kopierer und Multifunktionsgeräte.*

Die Absicherung der Fernwartung von VS-IT wird in der Anforderung CON.11.1.A18 *Fernwartung von VS-IT nach § 3 Abs. 3 VSA (B)* behandelt.

Dienstleistende

Hinsichtlich der Nutzung von Dienstleistenden, die (Cloud-)Plattformen für die VS-Verarbeitung bereitstellen, ist folgendes zu beachten:

- Die Dienstleistenden müssen für einen geeigneten Zugangs- und Zugriffsschutz innerhalb seines Zuständigkeitsbereich sorgen und muss den Bedarfsträger auf Anfrage entsprechende Dokumente und Nachweise zur Verfügung stellen.
- Der Bedarfsträger muss für seinen Zuständigkeitsbereich geeignete Maßnahmen zum Zugangs- und Zugriffsschutz implementieren. Hierbei reicht es nicht aus, sich auf den Schutz, den die Dienstleistenden bereit stellen, zu verlassen.
- Aus den Unterlagen muss das Ineinandergreifen des Zugangs- und Zugriffsschutzes zwischen den Maßnahmen der Dienstleistenden und des Bedarfsträgers deutlich werden.

In diesem Fall sind je nach Rolle die Ergebnisse der IT-Grundschutz-Checks der Bausteine OPS.2.3 *Nutzung von Outsourcing* oder OPS.3.2 *Anbieten von Outsourcing* zu berücksichtigen.

Zur Umsetzung dieser Anforderung empfiehlt sich der Verweis auf bestehende Konzepte ergänzt um eine Darstellung, wie diese ineinandergreifen. Ohne eine übergreifende Betrachtung des Zugangs- und Zugriffsschutz kann diese Anforderung nicht erfüllt werden.

Diese Anforderung ist sehr generisch gehalten, benötigt erfahrungsgemäß aber eine sehr detaillierte Ausarbeitung.

CON.11.1.M15 Handhabung von Datenträgern und IT-Produkten nach § 54 und Anlage V zur VSA (B)

Diese Anforderung befasst sich mit dem Umgang von Datenträgern und IT-Produkten, auf denen VS ungeschützt gespeichert werden. Dies bedeutet, dass die VS entweder unverschlüsselt oder durch ein IT-Produkt ohne Zulassungsaussage verschlüsselt wurden. In diesem Fall wird das IT-Produkt selbst zur VS und muss entsprechend geschützt werden.

Vorgehen

Zur Erfüllung dieser Anforderung sind im Regelfall organisatorische Maßnahmen sinnvoll. Da diese von den Geheimschutzbeauftragten festzulegen sind, sollten diese im Rahmen eines Interviews die folgenden Fragen beantworten können:

Wann? Wie oft?

- Wann und wie häufig werden die Mitarbeitenden sensibilisiert?

Wie?

- Gibt es organisatorische Vorgaben, wie mit als VS eingestuften IT-Produkten umgegangen wird?
- Werden die Mitarbeitenden im Umgang sensibilisiert?

Was?

- Welche Möglichkeiten stehen den Mitarbeitenden zur Verfügung, um eingestufte IT-Produkte VSA-konform aufzubewahren?

Zur Umsetzung dieser Anwendung kann das protokollierte Interview (nach BSI-Standard 200-2, Kapitel 8.4) mit den Geheimschutzbeauftragten verwendet oder auf entsprechende Dokumente verwiesen werden. Dokumente, auf welche verwiesen wird, sind beizufügen. Zusätzlich sollte darauf geachtet werden, dass die gewählten Maßnahmen dieser Anforderung und die Maßnahmen, die zur Umsetzung der Anforderungen

- CON.3.A12 *Sichere Aufbewahrung der Speichermedien für die Datensicherungen (B)*
- CON.7.A13 *Mitnahme notwendiger Daten und Datenträger (S),*
- SYS.3.1.A14 *Geeignete Aufbewahrung von Laptops (S)* und
- INF.7.A7 *Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger (S)*

ergriffen wurden, ineinandergreifen und sich sinnvoll ergänzen.

Da der Schutz der VS über den gesamten Lebenszyklus gewährleistet werden muss, ist u.a. ein Verweis auf die Aussonderung von eingestuften IT-Produkten nötig. Dies kann entweder in dieser Anforderung erfolgen oder es wird auf die Umsetzung der Anforderung CON.11.1.*A13 Löschung elektronischer VS, Vernichtung von Datenträgern und IT-Produkten nach §§ 32, 56 und Nr. 8 Anlage V zur VSA (B)* verwiesen. Zusätzlich ist auch die Anforderung CON.11.1.A9 *Speicherung elektronischer VS nach § 23 und Nr. 5 Anlage V zur VSA (B)* in diesem Kontext von Relevanz.

CON.11.1.M16 Zusammenschaltung von VS-IT nach § 58 VSA (B)

Unter Zusammenschaltung von VS-IT wird die direkte oder kaskadierte Verbindung von zwei oder mehr VS-IT-Systemen für die gemeinsame Nutzung von Daten und anderen Informationsressourcen (beispielsweise Kommunikation) bezeichnet.

Wenn zwei VS-IT-Systeme zusammen geschaltet werden, dann bleibt jedes VS-IT-System für sich eigenständig. Die Netzübergänge zwischen den zusammengeschalteten VS-IT-Systemen sind durch den Einsatz von IT-Sicherheitsprodukten mit Zulassungsaussage abzusichern. Es ist NICHT damit gemeint, dass durch die Zusammenschaltung der VS-IT-Systeme eine gemeinsame VS-IT entsteht. Stattdessen bedeutet dies nur, dass es möglich ist, Informationen von einem VS-IT-System zum anderen VS-IT-System übertragen zu können.

Voraussetzungen

Da nach § 58 VSA eine Zusammenschaltung zum Austausch von VS nur zwischen zwei oder mehreren VS-IT-Systemen erfolgen darf, ist darauf zu achten, dass bei einer Zusammenschaltung mit Nicht-VS-IT folgende Punkte beachtet werden:

- Der Verbindungsaufbau darf nur unidirektional von VS-IT-Systemen zur Nicht-VS-IT erfolgen.

- Es dürfen weder bewusst noch unbewusst VS in der NICHT-VS-IT gespeichert oder verarbeitet werden.
- Falls eine Nicht-VS-IT als Transportnetz verwendet werden soll, um VS-IT-Systeme zusammenzuschalten, dann ist die Übertragung der VS über das Transportnetz entsprechend zu schützen. (vgl. CON.11.1.A10 *Elektronische Übertragung von VS nach §§ 24, 53, 55 und Nr. 6.2 Anlage V zur VSA (B)*).

Vorgehen

Es ist empfehlenswert, eine Liste mit allen vorhanden und geplanten Kommunikationsverbindungen der VS-IT nach außen aufzustellen. Für jede Verbindung sollte ermittelt werden, ob darüber VS ausgetauscht werden sollen. Dabei helfen folgende Fragestellungen:

Was?

- Welche Kommunikationsverbindungen nach außen gibt es?
- Werden zum Schutz der Netzübergänge entsprechende IT-Sicherheitsprodukte mit Zulassungsaussage verwendet?
    - Falls nein, müssen zusätzliche IT-Sicherheitsfunktionen implementiert werden?

Wo?

- Wo kommt es zu Zusammenschaltungen, die betrachtet werden müssen?

Für jede Verbindung, für die das zutrifft, ist vor einem erstmaligen Austausch von VS eine Prüfung durchzuführen, ob Informationen zwischen den VS-IT-Systemen darüber ausgetauscht werden dürfen. Für diese Prüfung ist die Durchführung einer Gefahrenanalyse bzw. Risikoanalyse erforderlich, bei der die nachfolgenden Fragen zu klären sind:

Wer?

- Wer nutzt die jeweiligen VS-IT-Systeme?
- Welche Dienststelle trägt welche Verantwortung bzw. hat welche Zuständigkeit?

Wo?

- Wo befinden sich Schnittstellen/Systemübergänze zwischen den jeweiligen VS-IT-Systemen?

Wann? Wie oft?

- Sollen die VS-IT-Systeme nur temporär oder dauerhaft zusammen geschaltet werden?

Wie?

- Dürfen zwischen den zusammen geschalteten Systemen VS ausgetauscht werden?
    - Haben beide Systeme das gleiche Schutzniveau?
    - Kann die Einhaltung des Grundsatzes „Kenntnis nur, wenn nötig“ eingehalten werden?
- Sind die beiden VS-IT direkt zusammen geschaltet oder über ein Transportnetz?
    - Ist das Transportnetz ggf. auch für die Verarbeitung von VS des Geheimhaltungsgrades VS-NfD freigegeben?
    - Falls das Transportnetz nicht freigegeben ist, wie wird der Schutz der VS gewährleistet?
- Welche Zugriffsrichtung soll ermöglicht werden?
    - Unidirektional
    - Bidirektional

Was?

- Sollen VS zwischen den VS-IT-Systemen ausgetauscht werden?

- Welche Freigabe haben die einzelnen Systeme?
- Entsteht durch die Zusammenschaltung u.U. eine Zusammenstellung von VS (vgl. Anlage III zur VSA)?

Warum?

- Warum sollen die VS-IT-Systeme zusammengeschaltet werden?

Zur Umsetzung dieser Anforderung empfiehlt es sich, sowohl den Netzplan, als auch die Umsetzung des Bausteins NET.1.1 *Netzarchitektur und -design* zu berücksichtigen. Innerhalb des Bausteins CON.11.1 sind die Anforderungen:

- CON.11.1.A3 *Einsatz von IT-Sicherheitsfunktionen nach §§ 51, 52 VSA (B)*,
- CON.11.1.A4 *Beschaffung von VS-IT nach § 49 VSA (B*) und
- CON.11.1.A10 *Elektronische Übertragung von VS nach §§ 24, 53, 55 und Nr. 6.2 Anlage V zur VSA (B)* relevant.

Wird der Betrieb durch Dritte durchgeführt, sollte der Baustein OPS.3.2 *Anbieten von Outsourcing* und insbesondere die Anforderung OPS.3.2.A13 *Anbindung an die Netze der Outsourcing-Partner (S)* berücksichtigt werden. Es wird erwartet, dass dargelegt wird, ob und wo es im betrachteten Informationsverbund zu einer Zusammenschaltung kommt. In diesen Fällen sollten die Ergebnisse der Prüfung der Zusammenschaltung nach § 58 VSA beigefügt werden.

CON.11.1.M17 Wartungs- und Instandsetzungsarbeiten von VS-IT nach § 3 Abs. 3 VSA (B)

Auch bei einer VS-IT fallen eine Vielzahl an verschiedenen Wartungs- und Instandsetzungsarbeiten an. Wartungsarbeiten sind Arbeiten an einer funktionierenden VS-IT. Dazu gehört beispielsweise:

- (Firmware-)Aktualisierung von Hardware,
- Erweitern und Anpassen von Netze,
- Ausrollen neuer Software,
- Aktualisieren von Software sowie
- allgemeine Administrationstätigkeiten.

Instandsetzungsarbeiten sind hingegen Reparaturarbeiten an der VS-IT wie beispielsweise:

- Austausch (defekter) Hardware sowie
- Fehlersuche und Fehlerbehebung (beim Client/Server, im Netz etc.).

Aus Gründen der Übersichtlichkeit wird im Folgenden nur der Begriff "Wartung" verwendet.

Ziel

Das Ziel aus Geheimschutzsicht ist es, dass während dieser Tätigkeiten keine Dritte Kenntnis über VS erlangen. Daher empfiehlt sich eine frühzeitige Abstimmung zwischen dem Geheimschutz- und Informationssicherheitsbeauftragten.

Vorgehen

In Zusammenarbeit mit den zuständigen Administratoren und ggfs. weiteren verantwortlichen Personen sollten zuerst verschiedene Anwendungsfälle definiert und beschrieben werden, welche die verschiedenen Arten von Wartungs- und Instandsetzungsarbeiten einzeln abdecken. Dabei sollten auch die folgenden übergeordneten Fragen geklärt werden:

Was?

- Nach welchen Kriterien wird festgelegt, ob eine Wartung eine geheimschutzrelevante Änderung darstellt?

Wann?

- Wann werden die Geheimschutzbeauftragten über anstehende Wartungen informiert? (Zeitpunkt, Regelmäßigkeit)

Wie?

- Wie werden Mitarbeitende über anstehende Wartungs- und Instandsetzungsarbeiten informiert?
- Falls die Hardware nicht vor Ort gewartet werden kann, wie wird verhindert, dass VS die Einsatzumgebung verlassen?
- Wie wird mit geheimschutzrelevanten Änderungen umgegangen?
- Wie wird mit ausgesonderten Datenträgern oder anderen Komponenten verfahren (Bildtrommel, Thermoband etc.)?

In einem zweiten Schritt sollte durch alle Beteiligten für jeden Anwendungsfall festgelegt werden, wie die VS geschützt werden. Die umzusetzenden Maßnahmen und Möglichkeiten zur Einhaltung der Vorgaben hängen wesentlich von dem jeweiligen Anwendungsfall ab. Die nachfolgend aufgeführten Fragen sind als Leitfaden gedacht und sind pro Anwendungsfall im jeweiligen Kontext zu betrachten:

Wer?

- Wer führt die Wartung an VS-IT durch?
    - Handelt es sich um internes oder externes Personal?
    - Ist das Personal verpflichtet?
- Wer überwacht, genehmigt und beaufsichtigt die Wartung?
- Wer kontrolliert, dass die Wartung fachgerecht durchgeführt wurde?

Wo?

- Von wo wird auf die VS-IT zugegriffen?
- Wo wird die Wartung durchgeführt? (Inhouse, Extern)
- Worauf wird zugegriffen?
- Wo befinden sich VS im System?
- Wo könnten Angriffe stattfinden?
- Wo könnten VS abfließen?

Was?

- Welche Teilkomponenten der VS-IT werden gewartet?
- Was ist das Ziel der Wartung?
- Welche Tätigkeiten umfasst die Wartung von VS-IT?
- Was wird durch die Wartung verändert?
- Werden durch die Wartung geheimschutzrelevante Änderungen am System auftreten?

Wann?

- Wann werden diese Wartungen durchgeführt? (Bei Incident oder regelmäßig?)
- Wie häufig finden diese Wartungen an der VS-IT statt?
- Wie lange dauern diese Wartungen erfahrungsgemäß?
- Zu welchen Uhrzeiten finden diese Wartungsarbeiten statt?

- Müssen Systemteile temporär gekapselt werden bzw. stehen diese dann nicht zur Verfügung?
    - Falls Teile der VS-IT während der Wartung abgeschaltet werden müssen, wie lange sind diese nicht verfügbar?
- Kommt es zu Ausfallzeiten des Gesamtsystems?

Wie?

- Wie wird auf VS-IT zugegriffen? (Protokolle, Software, Endgeräte)
- Wie wird der unauthorisierte Zugriff auf VS während der Wartung verhindert?
    - Werden diese Zugriffe protokolliert?
    - Wird das Vier-Augenprinzip angewendet?
- Wie werden die VS während der Wartung im betroffenen Bereich geschützt?
- Wie sind genutzte Verbindungen abgesichert? (Bspw. Zugriff vom Admin-Client)
- Werden die Wartungen dokumentiert?

Warum?

- Warum wird die Wartung durchgeführt?

Wird Software gewartet, dann sollten die folgenden ergänzenden Fragen mitbetrachtet werden:

Wie?

- Wie kommen Zustands- oder Fehlerinformationen aus dem System raus (Protokolldaten)?
    - Wie werden dabei die Exporte um einen möglichen VS-Anteil bereinigt?
- Wie kommen Updates / neue Softwareanteile auf das System drauf?
- Wie wird die Integrität der Software gewährleistet?

Zur Ausgestaltung der Anwendungsfälle kann es hilfreich sein, auf den Umsetzungsbeschreibungen der Bausteine OPS.1.1.2: *Ordnungsgemäße IT-Administration* und OPS.1.1.3 *Patch- und Änderungsmanagement* aufzubauen. Falls die Wartung auch aus der Ferne durchgeführt werden soll, ist zusätzlich die Anforderung CON.11.1.A18 *Fernwartung von VS-IT nach § 3 Abs. 3 VSA (B)* zu berücksichtigen.

CON.11.1.M18 Fernwartung von VS-IT nach § 3 Abs. 3 VSA (B)

Mit dem Begriff Fernwartung wird - in Anlehnung an die Definition im Baustein OPS.1.2.5 *Fernwartung* - ein Zugriff auf VS-IT-Systeme und die darauf laufenden Anwendungen bezeichnet, der von einem anderen IT-System aus erfolgt. Der Arbeitsplatz, aus dem die Fernwartung heraus erfolgt, kann sowohl in der eigenen VS-IT als auch in einer fremden VS-IT liegen. Grundsätzlich ist die Fernwartung von VS-IT auf das notwendige Minimum zu begrenzen und nur dann durchzuführen, wenn es keine anderen Möglichkeiten gibt.

Durch Fernwartungen werden Verbindung von oder zu anderen Netzen geschaffen, wodurch besondere Risiken für die VS-IT entstehen. Zusätzlich zu den Überlegungen zur Wartung und Instandsetzung von VS-IT müssen daher ergänzende Maßnahmen zum Schutz der VS getroffen werden. Falls die Fernwartung nicht aus derselben VS-IT heraus erfolgt, so ist neben der zu wartenden VS-IT auch das Übertragungsnetz und die IT, aus der heraus administriert wird, als VS-IT zu behandeln und entsprechend abzusichern.

Vorgehen

Es sollten die folgenden Fragen im Rahmen der Überlegungen zur Fernwartung von VS-IT betrachtet werden:

Wer?

- Wer entscheidet, ob eine Fernwartung erforderlich ist?
- Wer führt die Fernwartung durch?
    - Internes Personal? (z. B. für IT im Homeoffice)
    - Externes Personal?
    - Ist das Personal verpflichtet?
- Wer überwacht die Durchführung der Fernwartung?

Wo?

- Von wo aus wird die Fernwartung durchgeführt?
- Worauf wird zugegriffen (Netzbereiche)?
- Welche Angriffsszenarien ergeben sich speziell aus der Fernwartung (Abfluss von VS)?

Was?

- Welche Teilkomponenten der VS-IT werden durch Fernwartung gewartet (Hardware/Software)?
- Ist die für die Administration genutzte IT als Schutzobjekt definiert?
- Welche Systemanteile müssen/dürfen per Fernwartung gewartet werden?

Wann?

- Wie häufig wird die Fernwartung der VS-IT durchgeführt?

Wie?

- Wie wird die Fernwartung überwacht und protokolliert?
- Erfolgt der Verbindungsauf und –abbau durch die Dienststelle?
- Kann die Verbindung jederzeit durch die Dienststelle unterbrochen werden?
- Wie ist die Verbindung abgesichert?
    - Ist die Datenübertragung durch ein IT-Sicherheitsprodukt mit Zulassungsaussage verschlüsselt? Wenn ja, durch welches?

Warum?

- Warum wird eine Fernwartung notwendig?
- Für welche Anwendungsfälle ist die Fernwartung erforderlich?

Ein weiterer Aspekt ist der Umgang mit nicht verpflichteten Fremdpersonal, das die Fernwartung durchführen soll. Es muss sichergestellt werden, dass deren Arbeiten überwacht werden und jederzeit die Möglichkeit besteht, die Fernwartung zu unterbrechen oder zu übernehmen.

Da diese Anforderung auf dem Baustein OPS.1.2.5 *Fernwartung* aufbaut, empfiehlt es sich, auf diesen Ergebnissen aufzusetzen. Je genauer die Fragen beantwortet werden und je präziser die Vorgaben formuliert sind, desto einfacher wird die Konzeption bzw. Erweiterung eines Konzepts für die Fernwartung von VS-IT.

3. Weiterführende Informationen

3.1. Wissenswertes

Hier werden ergänzende Informationen aufgeführt, die im Rahmen der Maßnahmen keinen Platz finden, aber dennoch beachtenswert sind. Derzeit liegen für diesen Baustein keine entsprechenden

Informationen vor. Sachdienliche Hinweise nimmt die IT-Grundschutz-Hotline gerne unter grundschutz@bsi.bund.de entgegen.

3.2. Quellenverweise

[BSI Schrift 7164] Liste der zugelassenen IT-Sicherheitsprodukte und –systeme, BSI, https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Zulassung/Liste-zugelassener-Produkte/liste-zugelassener-produkte_node.html

[BSI TL – IT 01] Mitwirkungspflichten im Zulassungsverfahren, BSI, https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Zulassung/BSI-TL-IT-01/BSI_TL_IT01_node.html

[BSI TL – M 50] Löschen und Vernichten von Verschlusssachen auf Datenträgern, BSI, https://www.bsi.bund.de/DE/Intern/Sicherheitsberatung/Bund/TechnischeLeitlinienVSA/TechnischeLeitlinienVSA_node.html

[REG-R] Registraturrichtlinie für das Bearbeiten und Verwalten von Schriftgut in Bundesministerien, BMI, 11.07.2001, https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/ministerium/registraturrichtlinie.html, letzter Abruf 10.07.2023

[VS-Produktkatalog] Katalog von Produktklassen und –Typen gemäß VSA, BSI, https://www.bsi.bund.de/dok/14127148

Merkblatt für den Umgang mit mobiler Informationstechnik bei Mitnahme ins Ausland, BSI, https://www.bsi.bund.de/DE/Intern/Sicherheitsberatung/Bund/Publikationen/InfoSichAusland/InfoSichAusland_node.html