

Häufig gestellte Fragen (FAQ) über die Nutzung von Informationstechnik im Bereich VS-NUR FÜR DEN DIENSTGEBRAUCH (zu Anlage 4 GHB – VS-NfD-Merkblatt)

Disclaimer

Vor der Weitergabe von Verschlusssachen (VS) des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD) an nichtöffentliche Stellen (u.a. Unternehmen) muss mit diesen jeweils ein Vertrag geschlossen werden, in den die Bestimmungen dieses VS-NfD-Merkblatts (Anlage 4 zum Handbuch für den Geheimschutz in der Wirtschaft, Geheimschutzhandbuch – GHB, Inkrafttreten 01.09.2023) Eingang gefunden haben. Die konkreten geheimschutzrechtlichen Anforderungen eines VS-NfD-Auftrages sind zwischen VS-NfD-Auftraggeber und VS-NfD-Auftragnehmer zu klären.

Die Inhalte dieser Fragensammlung wurden mit größter Sorgfalt und nach bestem Wissen erstellt. Für die Richtigkeit, Vollständigkeit und Aktualität der Inhalte kann jedoch keine Gewähr übernommen werden. Maßgeblich bleibt der Text des VS-NfD-Merkblattes bzw. wie er in den jeweiligen Vertrag zwischen VS-NfD-(Unter-) Auftraggeber und VS-NfD-(Unter-) Auftragnehmer Eingang gefunden hat.

Diese FAQ dienen nicht der Erörterung von Rechtsfragen und stellen keine rechtsverbindliche Auskunft dar, sondern dienen der unverbindlichen Erklärung wiederkehrender Fragemuster. I. Ü. ersetzen die FAQ keine Rechtsberatung oder die Klärung von Fragen zwischen VS-NfD-(Unter-) Auftraggeber und VS-NfD-(Unter-) Auftragnehmer. Andere Regelungen bleiben unberührt.

Stand: November 2023, Ergänzung/Überarbeitung dieses Dokumentes erfolgt bedarfsweise.

Allgemeine Fragen

An wen wende ich mich bei Rückfragen zu VS-NfD?

- Wenn Ihre Fragen nicht durch die Lektüre des VS-NfD-Merkblattes und die vorliegenden FAQ beantwortet werden können, wenden Sie sich für weitere Auskünfte an Ihren VS-NfD-Auftraggeber. VS-NfD-Unterauftragnehmer wenden sich an ihren VS-NfD-Unterauftraggeber.

Wurden bei der Erstellung des VS-NfD-Merkblattes, das zum 01.09.2023 in Kraft getreten ist, die Belange der Wirtschaft berücksichtigt?

- Ja, das BMWK hat die Wirtschaft bei der Erstellung beteiligt (Besprechungen, Stellungnahme), damit die Belange der Wirtschaft artikuliert werden konnten. Bei der Abstimmung des Merkblattes mit anderen Behörden hat das BMWK die Belange der Wirtschaft geltend gemacht. Zudem wurden die Rückmeldungen und Fragen aus der Wirtschaft in dem vorliegenden Dokument berücksichtigt.

Wurden die Belange von kleinen und mittleren Unternehmen (KMU) berücksichtigt?

- Ja, ein sog. KMU-Check wurde durchgeführt. Insbesondere die gestuften und differenzierenden Regelungen zum BSI-IT-Grundschutz und zur Selbstakkreditierung gehen hierauf zurück.

Geht das VS-NfD-Merkblatt über die Anforderungen der Allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlussachenanweisung – VSA) hinaus?

- Nein, das Merkblatt stellt ein vergleichbares Sicherheitsniveau zur VSA unter Berücksichtigung der Besonderheiten des VS-NfD-Schutzes in nichtöffentlichen Stellen her. Beispielsweise bedarf es nach dem VS-NfD-Merkblatt nicht in jedem Falle einer Umsetzung des BSI-IT-Grundschutzes.

Welche Vorgaben habe ich bei Nutzung von IT (Informationstechnik) beim Umgang mit VS-NfD einzuhalten?

- Bei Nutzung von IT beim Umgang mit VS-NfD ist neben den weiterhin anwendbaren Teilen des VS-NfD-Merkblattes zusätzlich Teil 3 dieses Merkblattes einzuhalten.

Welcher Weg ist der derzeit wohl üblicherweise kostengünstigste zur Bearbeitung von VS-NfD auf IT?

- Wenn eine VS-NfD Bearbeitung nur in geringem Umfang stattfindet, stellt ein Einzelplatzsystem (sog. Stand Alone Gerät) den derzeit wohl kostengünstigsten Fall dar

Welche Vorgaben habe ich einzuhalten, wenn ich vergleichbar VS-NfD eingestufte internationale VS (z. B. NATO RESTRICTED, OCCAR RESTRICTED, etc.) bearbeite?

- Bei der Verarbeitung von VS über- oder zwischenstaatlicher Einrichtungen und Stellen eines mit VS-NfD vergleichbaren Geheimhaltungsgrades gelten die jeweiligen Vorschriften/vertraglichen Vereinbarungen dieser Einrichtungen/Stellen. Fragen hierzu sind entlang der „Linie der Beauftragung“ zu klären.

Warum sieht das VS-NfD-Merkblatt den Hinweis auf eine mögliche Strafbarkeit nach den §§ 93ff StGB vor?

- Auch eine VS-NfD kann ein Staatsgeheimnis i.S.d. § 93 StGB darstellen (sog. materieller Staatsgeheimnisbegriff). Auf die Einstufung kommt es dabei nicht zwingend an. Die Einstufung auf Grundlage des SÜG bzw. der VSA hat hinsichtlich des Vorliegens eines Staatsgeheimnisses lediglich Indizwirkung. Eine Strafbarkeit nach den §§ 93ff StGB ist daher auch für VS-NfD denkbar.

Gibt es eine Übersetzung des VS-NfD-Merkblattes in andere Sprachen?

- Eine englischsprachige, rechtlich unverbindliche Höflichkeitsübersetzung (sog. courtesy translation) steht im Sicherheitsforum des BMWK zum Download bereit.

Welche Vorgaben habe ich einzuhalten, wenn ich vergleichbar VS-NfD eingestufte ausländische VS bearbeite?

- Die Regelungen des VS-NfD-Merkblattes gelten für deutsche VS-NfD sowie für ausländische vergleichbar eingestufte VS, die einem Unternehmen in Deutschland zur Aufbewahrung oder Verarbeitung auf Grundlage eines bilateralen Geheimschutzabkommens (GSA) überlassen worden sind. Ggf. sind weitere Vorgaben sind zu beachten.

Ist eine Bearbeitung von VS-NfD in Papierform im Homeoffice möglich?

- Eine Mitnahme zur Verarbeitung von VS-NfD in Papierform ist in der Privatwohnung grundsätzlich unzulässig. Jedoch kann der öffentlicher VS-NfD-Auftraggeber Ausnahmen zulassen (siehe Teil 2, Ziff. 7). Darauf bezieht sich auch der Hinweis in Teil 6, Ziff. 2.

Besteht die Möglichkeit einer Sicherheitsüberprüfung (SÜ) für VS-NfD verpflichtetes Personal (z.B. Administratoren)?

- Nein. Die rechtliche Grundlage ist das Sicherheitsüberprüfungsgesetz (SÜG). Dieses erlaubt eine SÜ erst beim Umgang mit Verschlusssachen ab dem Geheimhaltungsgrad VS-VERTRAULICH.

Erhalte ich für VS-NfD einen Sicherheitsbescheid?

- Nein, für den Geheimhaltungsgrad VS-NfD wird kein Sicherheitsbescheid ausgestellt.

Kann ich für VS-NfD eine Facility Security Clearance (FSC) erhalten?

- Nein, für den Geheimhaltungsgrad VS-NfD wird keine FSC ausgestellt.

Welche Person aus dem Unternehmen hat Teil 1b) des Merkblattes (Vereinbarung) zu unterschreiben?

- Das Unternehmen bestimmt, wer die Unterschrift leistet. Erforderlich ist jedoch, dass die unterzeichnende Person zu diesem Zeitpunkt hierfür die erforderlich Vertretungsmacht hat.

Kann der VS-NfD-Auftraggeber weitere Anforderungen, die über die im VS-NfD-Merkblatt benannten Anforderungen hinausgehen, verlangen?

- Ja, der VS-NfD-Auftraggeber kann im Einzelfall auf vertraglicher Basis über das VS-NfD-Merkblatt hinausgehende Anforderungen in eigener Verantwortung vereinbaren.

Soll das neue Merkblatt weiterentwickelt werden?

- Eine Evaluierung des neuen VS-NfD-Merkblattes erfolgt zu gegebener Zeit. Der technische Fortschritt, insbesondere im VS-NfD-IT-Bereich, und die sich stetig verändernde Sicherheitslage werden es erforderlich machen, auch das neue VS-NfD-Merkblatt daran angepasst weiterzuentwickeln. Hierbei wird die Wirtschaft erneut beteiligt und deren Belange berücksichtigt werden.

Anwendungsfragen zur Verarbeitung von VS-NfD auf IT

Allgemeine Anwendungsfragen

Ich möchte VS-NfD auf IT bearbeiten. Welcher Weg ist der derzeit wohl üblicherweise kostengünstigste?

- Wenn eine VS-NfD Bearbeitung nur in geringem Umfang stattfindet, stellt ein Einzelplatzsystem (sog. Stand Alone Gerät) den derzeit wohl regelmäßig kostengünstigsten Fall dar.

Kann ich für mein VS-NfD Netz beim BMWK eine Genehmigung bekommen?

- Nein, für den Schutz von VS-NfD ist nach dem Geheimschutzhandbuch (GHB) ausschließlich die für VS-NfD benannte verantwortliche Person des Unternehmens zuständig.

Ist eine (Teil-) Auslagerung der IT-Administration im Bereich VS-NfD zulässig?

- Die VS-NfD-IT-Administration ist grundsätzlich durch eigenes Personal auszuführen. Ein allgemeines Auslagern der VS-NfD-IT-Administration ist unzulässig.

Was muss ich beachten, wenn ich verschiedene VS-NfD-Projekte bearbeiten möchte?

- Daten unterschiedlicher VS-NfD-Aufträge müssen jeweils in separaten und ausschließlich für die jeweiligen zugriffsberechtigten Nutzer freigegebenen Projektordnern abgelegt werden. Seitens des Auftraggebers können weitergehende Anforderungen, bspw. ausschließliche Verwendung des IT-Systems für das jeweilige Projekt gefordert werden.

Kann ich auch meinen dienstlichen Tablet-PC oder mein Smartphone als mobiles IT-System für VS-NfD einsetzen?

- Ja, grundsätzlich besteht die Möglichkeit. Dies erfordert die Umsetzung der Anforderungen gemäß VS-NfD-Merkblatt, sowie einer Freigabe der für VS-NfD verantwortlichen Person.

Können die VS-NfD-IT-Systeme an beliebigen Orten im Unternehmen betrieben werden?

- Räumliche Arbeitsbereiche müssen durch die VS-NfD verantwortliche Person zuvor freigegeben werden. Der Grundsatz „Kenntnis, nur wenn nötig“ muss durch geeignete Maßnahmen (z.B. abschließbare Behältnisse, Sichtschutz), sichergestellt werden.

Müssen Datenserver bzw. in der Produktion verwendete Maschinen, auf welche sich Daten mit VS-NfD-Inhalt befinden täglich ausgeschaltet werden, wie Einzelplatz Systeme gem. Teil 3, Ziff. 2.1.1?

- Nein, Server müssen nicht arbeitstäglich ausgeschaltet werden, wenn die betreffenden Vorgaben nach Teil 2, Ziff. 5 eingehalten werden. Gleiches gilt für VS-NfD verarbeitende Maschinen welche aufgrund von z.B. Dauerbetrieb, Rüstzeiten etc. nicht arbeitstäglich ausgeschaltet werden können.

Mein Rechner stürzt aufgrund eines Defekts im laufenden Betrieb ab. Auf dem Datenträger befinden sich eingestufte Daten. Ich kann diese aber vor der Wartung / Reparatur nicht löschen. Was muss ich tun?

- Auf Datenträgern, die VS-NfD unverschlüsselt enthalten, sind die VS-NfD komplett zu löschen, bevor die Datenträger im Rahmen von Wartungs- oder Reparaturarbeiten am IT-System den persönlichen Gewahrsam der zugriffsberechtigten Personen verlassen. Ist eine

VS-NfD-FAQ

Löschung nicht möglich, sind die Datenträger auszubauen und zurückzuhalten. Ist das nicht möglich, gilt Teil 2, dieses Merkblattes.

Ich möchte VS-NfD-Daten im Unternehmensnetz, in einem separaten, passwortgeschützten Ordner ablegen. Auf diesen Ordner haben nur die VS-NfD verpflichteten Personen Zugriff. Eine Firewall wird im Unternehmensnetz eingesetzt. Entspricht dieses Vorgehen den Anforderungen?

- Nein. Hier handelt es sich nicht um ein separiertes VS-IT-System („air-gapped“). Demzufolge müssen sämtliche Anforderungen zur Kopplung eines VS-NfD-Netzes mit einem Netzwerk mit niedrigerem Sicherheitsniveau umgesetzt werden.

Ich möchte private Peripheriegeräte an meinem VS-Nf- Laptop verwenden, ist dies möglich?

- Nein, private Geräte dürfen grundsätzlich nicht für die Verarbeitung von Verschlusssachen eingesetzt werden.

Darf ich in meinem IT-System eine Funk-Tastatur und eine Funk-Maus einsetzen?

- Sofern diese über eine Zulassungsaussage des BSI verfügen, ist dies zulässig. Derzeit stehen jedoch keine Produkte mit einer solchen Aussage zur Verfügung.

Darf zur Bearbeitung von VS-NfD-Daten eine WLAN-Verbindung genutzt werden?

- Die WLAN-Nutzung ist bei der Bearbeitung von VS-NfD nur in Verbindung mit einer Virtual Private Network (VPN) Lösung gestattet, welche über eine Zulassungsaussage des BSI verfügt. Entsprechende Produkte finden Sie auf der Webseite des BSI.

Darf ich VS-NfD aus dem Homeoffice elektronisch bearbeiten?

- Obligatorisch sind zunächst weiterhin die Anforderungen des VS-NfD-Merkblattes sowie die spezifischen Einsatz- und Betriebsbedingungen der eingesetzten BSI-Produkte mit Zulassungsaussage umzusetzen. Zusätzliche Regeln sind einzuhalten:
 - die genutzte IT (z. B. Notebooks) hierfür von der für VS-NfD verantwortlichen Person freigegeben ist,
 - sich die Privatwohnung innerhalb Deutschlands befindet,
 - die für VS-NfD verantwortliche Person ihre Zustimmung erteilt hat,
 - der/die Mitarbeiter/in über spezifische Risiken des mobilen Arbeitens belehrt ist und
 - Teil 6 des Merkblattes von dem/der Mitarbeiter/in unterzeichnet wurde und vom Unternehmen als Nachweis aufbewahrt wird.

BSI-IT-Grundschutz und Selbstakkreditierung

Findet der IT-Grundschutz des BSI grundsätzlich Anwendung?

- Die Umsetzung des IT-Grundschutzes des BSI ist abhängig von der Ausprägung des VS-IT-Systems. Einzelplatzsysteme gem. VS-NfD-Merkblatt bleiben hiervon unberührt; hier sind ausschließlich die entsprechenden technischen und organisatorischen Maßnahmen zum Schutz der VS-NfD auf IT-Systemen gemäß VS-NfD-Merkblatt anzuwenden.

Wird für mein VS-NfD Netz eine Zertifizierung (z.B. ISO 27001) gefordert?

- Nein, die für VS-NfD verantwortliche Person im Unternehmen bestätigt der Geschäftsleitung spätestens alle drei Jahre schriftlich die Umsetzung der Anforderungen aus Teil 3 (IT-Anforderungen) dieses Merkblattes (Selbstakkreditierung).

Muss die Selbstakkreditierung durch einen BSI-zertifizierten BSI-IT-Grundschutz-Berater erfolgen?

- Nein, weder ist eine Zertifizierung erforderlich, noch müssen etwaig hinzugezogene Berater zertifiziert sein.

Darf ich mich bei der Umsetzung des BSI-IT-Grundschutzes beraten lassen?

- Ja. Der Berater muss auch kein BSI-zertifizierter BSI-IT-Grundschutz-Berater sein (s. o.). Die Selbstakkreditierung nimmt dennoch die verantwortliche Person vor. Bei Inanspruchnahme einer Beratung bleiben die Pflichten der verantwortlichen Person unberührt.

Welche Details muss die Selbstakkreditierung gemäß Merkblatt beinhalten?

- In der Selbstakkreditierung erklärt das Unternehmen die Umsetzung der IT-Anforderungen in der jeweils gültigen Fassung, sofern erforderlich, die Umsetzung der die Einsatz- und Betriebsbedingungen der Produkte mit Zulassungsaussage des BSI und die Beachtung des jeweils gültigen IT-Grundschutzes des BSI mit Erstellung eines Informationssicherheitskonzepts und einer Risikoanalyse, sofern erforderlich.

Wenn ich bereits ISO 27001 zertifiziert bin, gilt dann der BSI-IT-Grundschutz als erfüllt bzw. umgesetzt?

- Wenn die ISO 27001 Zertifizierung auf Basis des einschlägigen Dokumentendossiers des BSI-IT-Grundschutzes erfolgt, gilt der BSI-IT-Grundschutz als erfüllt bzw. umgesetzt. Für alle anderen Fälle muss eine Gegenüberstellung der Zertifizierungsdokumente (Differenzanalyse, sog. Gap-Analyse) erfolgen und ggf. nicht erfüllte Anforderungen des BSI-IT-Grundschutzes zusätzlich umgesetzt werden.

Wo finde ich Hilfe bei der Umsetzung des BSI-IT-Grundschutzes?

- Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt auf seinen Seiten hierzu umfangreiche, anwenderorientierte Informationen (u. a. Checklisten, Zuordnungstabelle, Migrations-Anleitung mit Tabellen, Hilfsmittel, fiktives Fallbeispiel zu einem mittelständischen Unternehmen, IT-Grundschutz-Profile) zur Verfügung.

Software

Dürfen VS-NfD Daten im Unternehmensnetz in einem virtualisierten Bereich / Umgebung abgelegt werden?

- Nein. Grundsätzlich sind VS-NfD-Daten in einer VS-NfD-konformen Umgebung gemäß den Vorgaben der Anlage 4 des GHB (VS-NfD-Merkblatt) vorzuhalten. Das Maß der technische sowie organisatorische Maßnahmen orientiert sich dabei an der Ausprägung des VS-IT-Systems, in welchem auch das Anlegen virtualisierter Bereiche möglich ist.

Welche Vorgaben gibt es bzgl. der Telemetriedaten-Übertragung?

- Für Betriebssysteme und mögliche weitere Applikationen (Software-Anwendungen) gilt, dass eine Telemetrie-Datenübertragung sowie weitere ungewollte Datenabflüsse von der eigentlichen VS-IT Bearbeitung auszuschließen sind und dies als fortlaufender Prozess zu prüfen ist.

Kann ein Virenschanner mit einer online Datenprüfung im Bereich VS-NfD eingesetzt werden?

- Nein, eine solche Software darf nur eingesetzt werden, wenn sich der Upload von Daten nachweislich deaktivieren lässt. Die Funktionalität ist nach jedem Update der Software zu prüfen.

Kryptierung

Allgemeines zur Kryptierung

Was gilt es zu verschlüsseln?

- Verschlüsselt werden muss entweder die Hardware selbst mit einer geeigneten Festplattenverschlüsselung und/oder die elektronische Übermittlung der Daten durch Produkte, welche über eine Zulassungsaussage des BSI verfügen.

Wir verwenden eine Verschlüsselungssoftware zum elektronischen Datenversand. Kann dieses Produkt auch zum Versand von VS-NfD eingesetzt werden?

- Ja, sofern das Produkt über eine Zulassungsaussage des BSI verfügt.

Wo finde ich die zugelassenen Kryptosysteme?

- Eine abschließende Auflistung aller Kryptosysteme mit BSI-Zulassungsaussage finden Sie auf der Webseite des BSI. Die entsprechenden Einsatz- und Betriebsbedingungen zu den Produkten können aus dem Sicherheitsforum des BMWK - Geheimschutzservers (geschützter Bereich) heruntergeladen werden. Alle nicht geheimschutzbetreuten Unternehmen beziehen diese Dokumente über Ihren VS-Auftraggeber.

Kryptierung von Hardware

Warum brauche ich eine geeignete Festplattenverschlüsselung und warum reicht es nicht aus, dass auf meinem Notebook die Dateien oder Ordner, BSI-konform verschlüsselt abgelegt sind?

- Sofern auf einem Datenträger alle VS-NfD-Dateien ordnungsgemäß BSI-konform verschlüsselt sind, bedarf es keiner zusätzlichen Festplattenverschlüsselung. Diese Konstellation ergibt sich jedoch ausschließlich für den Anwendungsfall Datensicherung. Zur VS-IT-Bearbeitung benötigt man die VS-Daten jedoch im Klartext. Dabei kann es auch passieren, dass vom Betriebssystem VS-Daten temporär ausgelagert werden. Daher hat man selbst nach mehrmaligem nach den Vorgaben des BSI vorgenommenen Löschen keine Gewissheit, dass sich nicht doch noch VS-Daten in Klartext auf dem Notebook befinden. Des Weiteren gibt es im Umgang mit Datenträgern, welche auf einer Halbleiterphysik basieren (SSD, etc.), derzeit keine Löschräume mit Zulassungsaussage des BSI. Demzufolge sind Notebooks im mobilen Einsatz mit einer BSI-konformen Festplattenverschlüsselung zu versehen.

Muss ich meine CDs, USB-Sticks, Wechselplatten etc. auch verschlüsseln?

- Nein. VS-Datenträger, welche eingestufte Daten unverschlüsselt enthalten, sind jedoch generell den Vorschriften entsprechend zu kennzeichnen und im persönlichen Gewahrsam zu führen oder in verschlossenen Räumen / Behältnissen aufzubewahren.

Kryptierte Übertragung von Daten

Was bedeutet Übertragung von Daten i.S.d. Merkblatts?

- Eine kryptierte Übertragung von Daten ist immer dann erforderlich, wenn ein Zugriff durch Dritte über einen Leitungsweg bzw. Übertragungsmedium nicht ausgeschlossen werden kann. Bei einer campus- bzw. standortübergreifenden elektronischen Datenübertragung kann i.d.R. ein Zugriff durch Dritte nicht ausgeschlossen werden.

Gibt es Ausnahmen von der kryptierten Übertragung?

- Ja, wenn die Übertragung innerhalb einer Liegenschaft ausschließlich leitungsgebunden erfolgt und sämtliche Übertragungseinrichtungen, -leitungen, -verteiler und Trassen gegen unbefugten Zugriff geschützt sind, kann eine Verschlüsselung unterbleiben.

Ich greife von einem anderen Ort auf den Fileserver zu. Ist dies eine Übertragung?

- Ja, dies stellt eine elektronische Datenübertragung dar.

Was ist bei der Übertragung zu beachten?

- Die Daten sind mit Produkten zu verschlüsseln, welche über eine Zulassungsaussage des BSI verfügen.

Was ist die Alternative zur kryptierten Übertragung?

- Zum einen kann eine liegenschaftsübergreifende Übertragung von VS-Daten über nachweislich geschützte Leitungswege erfolgen. Zum anderen kann die VS per VS-Datenträger oder in Papierversion ausgetauscht werden. Hierbei sind die allgemeinen VS-Kennzeichnungs- und -Schutzpflichten einzuhalten.

Ich möchte VS-NfD als Anlage zu einer Mail versenden. Was muss ich beachten?

- Mailversand von VS-NfD ist nur in Form einer kryptierten Anlage erlaubt. Zur Kryptierung sind ausschließlich Produkte einzusetzen, welche über eine Zulassungsaussage des BSI verfügen. Eine aktuelle Auflistung solcher Produkte findet sich auf der Webseite des BSI. Der Versand von VS-NfD mit Verschlüsselung durch Produkte ohne Zulassungsaussage des BSI stellt ein Sicherheitsvorkommnis dar.

„isolierte Netze“ und Public Cloud

Anmerkungen zum Thema „isolierte Netze“

Mit zunehmender Vernetzung werden IT-Systeme immer anfälliger für Cyberangriffe. Angesichts dieser zunehmenden Bedrohungen rückt die Sicherheit von IT-Systemen immer stärker in den Fokus. Dazu zählt z.B. der weltweite Einsatz gleicher Hard- und Softwaresysteme aber auch die Varianz in den Lieferketten (supply chain). Dies führt zu einer erhöhten Bedrohungslage für die Kompromittierung von VS-NfD durch Schadsoftware. In diesem Zusammenhang wird darauf hingewiesen, dass die VS-NfD-Daten in speziell geschützten Datenbereichen vorzuhalten sind. Als weitergehenden Schutz der VS-NfD-Daten empfiehlt es sich regelmäßig, eine Trennung der VS-NfD-Daten vom Unternehmensnetzwerk („air-gapped“) herbeizuführen. Dies führt zu einer erheblichen Reduzierung der Gefährdungslage im Kontext Cyber Security und zugleich zur Reduzierung der VS-NfD-Administrationsaufwände.

Nutzung von Public Cloud-Diensten (gegenwärtig nicht gestattet)

Ist eine Ablage BSI-konform verschlüsselter Daten in einer Public Cloud erlaubt?

- Nein, eine Datenablage bei einem externen Serviceprovider bzw. in einer Public Cloud ist auch dann nicht erlaubt, wenn die Daten BSI-konform verschlüsselt wurden. Dies begründet sich wie folgt: In den Einsatz- & Betriebsbedingungen wird darauf hingewiesen, dass das Produkt in der zugelassenen Konfiguration kryptographische Mechanismen verwendet, die nicht quantencomputer-resistent sind. Der mögliche Einsatz von Künstlicher Intelligenz (KI) in einer Public Cloud und der damit einhergehende zusätzliche Gefährdungsgrad kann gegenwärtig nicht abgeschätzt werden, insbesondere vor dem Hintergrund einer Einstufungsdauer der zu schützenden VS-NfD von regelmäßig 30 Jahren. Des Weiteren erhält der Benutzer vor dem Entschlüsseln keinerlei Warnmeldungen, dass der Ablageort der VS-NfD in einem VS-NfD-konformen Bereich zu erfolgen hat. Ein Entschlüsseln in der Public Cloud kommt einem meldepflichtigen Sicherheitsvorfall gleich.

Dürfen Online-Programme benutzt werden, die auf die VS-NfD zugreifen müssen?

- Nein. Eine online-Bearbeitung von VS-NfD entspricht einer Bearbeitung von VS-NfD in einer Public Cloud.

Dürfen Private-Cloud Lösungen eingesetzt werden?

- Der VS-NfD-Auftragnehmer ist in seinen Räumlichkeiten (z.B. Rechenzentrum, Serverraum) berechtigt, eine Private Cloud Infrastruktur zu errichten und in Form von unternehmenseigenen IT-Administratoren zu betreiben. Im Übrigen gelten die Anforderungen gemäß Teil 3 VS-NfD Merkblatt.