Praxishandbuch

für die Handhabung von VS-NfD auf IT im Unternehmen

AKSIBE.NW

Inhalt

1 Vorwort

Dieses Praxishandbuch soll – wie der Name schon andeutet – für alle Verantwortlichen, die Umgang mit Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD) haben, eine Hilfestellung sein, legt jedoch den Schwerpunkt auf Verarbeitung in elektronischer Form. Das Handbuch richtet sich in erster Linie an VS-NfD-Verantwortliche in Unternehmen, die nicht geheimschutzbetreut sind und deshalb keinen vom BMWi bestellten Sicherheitsbevollmächtigten (SiBe) haben. Aber auch Sicherheitsverantwortliche von Unternehmen, die der Geheimschutzbetreuung des BMWi unterliegen, werden adressiert.

Entstanden ist das Praxishandbuch aus der Erkenntnis heraus, dass die aufsichtsbehördlichen Vorgaben zum Umgang mit VS-NfD in einer immer komplexer werdenden Unternehmens-IT nur dann erfolgreich umgesetzt werden können, wenn vorher ein Plan, also ein Konzept, erstellt wird, wie diese Umsetzung – orientiert an den speziellen Gegebenheiten der firmeneigenen IT – erfolgen soll.

Es geht also in diesem Handbuch im Wesentlichen nicht um die Frage, was umgesetzt werden soll, da die Anforderungen von der Aufsichtsbehörde kommen und im juristischen Sinne hinreichend klar sind. Vielmehr geht es um die „Übersetzung“ der juristischen Anforderungen in technisch/organisatorische „Anforderungen“, so wie sie in der Technik, insbesondere bei der Applikationsentwicklung, üblich sind.

Gleichwohl ließ es sich nicht ganz vermeiden, in Einzelfällen auch Erläuterungen zu den staatlichen Vorgaben – im Sinne juristischer Kommentare – abzugeben, um dem Umsetzungsverantwortlichen ein besseres Verständnis bei der Interpretation dieser Vorschriften zu ermöglichen.

Die Autoren möchten an dieser Stelle nicht versäumen, den Mitarbeitern des Bundesministeriums für Wirtschaft und Energie (BMWi) für ihre konstruktive Begleitung bei der Entstehung dieses Handbuchs zu danken. Ein ganz besonderer Dank gilt Herrn Thomas Königshofen, Deutsche Telekom, der die Idee des Handbuches an den Arbeitskreis der Sicherheitsbevollmächtigten in NRW herangetragen und dieses Projekt mit aus der Taufe gehoben hat.

Dieses Handbuch ist als „lebendes“ Dokument konzipiert. Genauso wie sich die Unternehmens-IT in einem laufenden Wandel befindet, soll das Handbuch nach und nach um weitere Kapitel, Hinweise und Hilfestellungen bei der Lösung von Einzelfragen ergänzt werden. Es lebt in seiner Aktualität also auch von der konstruktiven Kritik und dem Feedback seiner Nutzer. Deshalb sind Hinweise und Anregungen zur Verbesserung des Handbuchs an die Autoren jederzeit willkommen.

2 Einleitung

Die nachfolgenden Kapitel sind in ihrer Gliederung an die in Unternehmen übliche Form der Beschreibung von Geschäftsprozessen angelehnt, also einer Gliederung nach zeitlicher Abfolge.

Um auch den Sicherheits- und IT-Verantwortlichen, die erstmalig mit den Anforderungen zum Schutz von VERSCHLUSSSACHEN - NUR FÜR DEN DIENSTGEBRAUCH konfrontiert werden, eine Hilfestellung zu bieten, ist zunächst die Phase zu beschreiben, in der das Unternehmen erwägt, einen Auftrag mit VS-Relevanz anzunehmen, also vertragliche Verpflichtungen zur Umsetzung der staatlichen Anforderungen an den Schutz von VS-NfD einzugehen.

Im gesamten Dokument sind Hinweise auf die jeweils gültigen amtlichen Dokumente in der Form [*dokument-referenz*] zu finden, um die Orientierung zu erleichtern. In Abschnitt 11.1 befindet sich die vollständige Literaturangabe.

3 Allgemeine Grundsätze

Um die Vorschläge und Praxishinweise zur Umsetzung von VS-NfD in die Unternehmens-IT besser zu verstehen, bedarf es hinsichtlich der Zielsetzung der staatlichen Anforderungen einiger Erläuterungen oder Vorab-Bemerkungen, die ganz allgemein für alle nachfolgenden Kapitel als Richtschnur bzw. Rahmenvorgabe gelten. Diese sind als „Allgemeine Grundsätze“ normiert.

3.1 Grundsatz 1:

Kenntnis nur, wenn nötig

Eingestufte Informationen dürfen grundsätzlich nur Personen zugänglich gemacht werden, die diese für die Auftragsanbahnung oder die Auftragsdurchführung benötigen. Verschwiegenheit gegenüber Nichtbeteiligten ist zu wahren.

3.2 Grundsatz 2:

Bei der Behandlung von VS ist die Einstufung des VS-Auftraggebers maßgeblich

Bei der Definition von VS gilt zunächst die vertraglich verbindliche staatliche Einstufung. Das, was der VS-Auftraggeber als VS-NfD klassifiziert (einstuft), ist entsprechend so zu behandeln. Es ist insbesondere nicht die Aufgabe des VS-Auftragnehmers, die staatliche Einstufung anhand der gesetzlichen Definitionen (siehe § 4 Abs. 2 Nr. 4 [SÜG]) infrage zu stellen oder die VS einseitig einem anderen Geheimhaltungsgrad zuzuordnen. Weitere Informationen hierzu befinden sich in Kapitel 7.3.

3.3 Grundsatz 3:

Eine für VS-Vertraulich und höher ertüchtigte IT reicht für die Verarbeitung von VS-NfD aus; die vorhandene IT zur Umsetzung unternehmensinterner Vorgaben für die Behandlung streng vertraulicher Informationen und Geschäftsgeheimnisse reicht in der Regel nicht

IT-technisch und organisatorisch ist davon auszugehen, dass eine für eine höhere staatliche Schutzklasse (z.B. VS-VERTRAULICH) zugelassene IT-Umgebung immer auch für die Informationsverarbeitung von VS-NfD ausreicht.

Keinesfalls ist aber davon auszugehen, dass eine durch nicht staatliche, unternehmensinterne Informationsklassifizierung, beispielsweise „XY GmbH-vertraulich“, „XY GmbH-streng vertraulich“ oder „XY GmbH-Top Secret“, ertüchtigte IT-Umgebung auch für den Schutz von VS-NfD ausreicht. Die staatlichen Anforderungen an den Schutz von VS-NfD weichen mit hoher Wahrscheinlichkeit von den etablierten unternehmensinternen Anforderungen an die IT zum Schutz sensibler Daten und Geschäftsgeheimnisse ab.

3.4 Grundsatz 4:

Risikominimierung unbefugter Kenntnisnahme

Der Schutz von Verschlusssachen zielt darauf ab, das Risiko unbefugter Kenntnisnahme durch Dritte, mit negativen Folgen für den Staat, zu minimieren. In Bezug auf IT-Sicherheit steht im Geheimschutz das IT-Sicherheitsziel „Vertraulichkeit“ im Blickpunkt aller Maßnahmen, vorrangig vor den anderen Zielen „Verfügbarkeit“ und „Integrität“.

3.5 Grundsatz 5:

Schutzstandards für die VS-NfD-Verarbeitung in der IT müssen mindestens den Schutzstandards der VS-NfD-Dokumentenbehandlung in Papierform entsprechen

Aus der staatlichen Zielsetzung der Risikominimierung im Hinblick auf Vertraulichkeitsverletzungen leitet sich der Grundsatz ab, dass die Schutzmaßnahmen in der IT mindestens die gleiche Schadensprävention leisten müssen, wie sie bei der Behandlung von VS in Papierform vorgeschrieben ist.

3.6 Grundsatz 6:

Bei der Umsetzung der Anforderungen an die informationstechnische Verarbeitung von VS-NfD sind ggf. zusätzliche vertragliche Anforderungen an die IT-Sicherheit zu berücksichtigen

Um alle vertraglich vereinbarten Anforderungen des VS-Auftraggebers zu erfüllen, reicht es in der Regel nicht aus, lediglich die Anforderungen, die sich aus der Einstufung „VS-NfD" ergeben, umzusetzen. Fallweise können VS-Auftraggeber weitere geheimschutz-, sabotageschutz- und sonstige sicherheitsrelevante Anforderungen vertraglich vereinbaren[1].

3.7 Grundsatz 7:

Mitarbeiter müssen nachweislich belehrt sein, bevor Sie Zugang zu VS-NfD haben dürfen oder sich diesen verschaffen können

Personen, die Zugang zu VS-NfD haben oder sich verschaffen können, müssen *nachweislich* über den Inhalt des VS-NfD-Merkblattes [VS-NfD-MB] belehrt worden sein. Die Belehrung muss auch auf die möglichen straf- bzw. vertragsrechtlichen Konsequenzen eingehen. Darüber hinausgehende Maßnahmen, beispielsweise die formale Aufnahme in die Geheimschutzbetreuung des Bundes, sind erst für höhere Auftragseinstufungen erforderlich.

3.8 Grundsatz 8:

VS-Zwischenmaterial

VS-Zwischenmaterial (z.B. Vorentwürfe, Stenogramme, Tonträger, Folien) ist gegen Einsichtnahme Unbefugter in derselben Weise zu schützen wie das Bezugsdokument. VS-Zwischenmaterial, das nicht an Dritte weitergegeben und unverzüglich vernichtet wird, muss nicht als VS gekennzeichnet werden.

3.9 Grundsatz 9:

Weitergabe von VS-NfD

Über den Inhalt der VS ist Verschwiegenheit gegenüber Nichtbeteiligten zu wahren. Vor Weitergabe von VS-NfD an Dritte ist die Einwilligung des amtlichen VS-Auftraggebers einzuholen. Weitere Informationen hierzu befinden sich in Kapitel 7.1.

---

[1] Auf Punkte wie Sicherheitsüberprüfungen aufgrund anderer Rechtsvorschriften (bspw. Satellitensicherheit, Atomgesetz, Luftsicherheit, Sabotageschutz, Ländergesetze ...) kann in diesem Praxishandbuch nicht weiter eingegangen werden.

3.10 Grundsatz 10:

Verlust, unbefugte Weitergabe, Auffinden von VS oder Nichtbeachtung des VS-NfD-Merkblattes

Der Verlust, die unbefugte Weitergabe sowie das Auffinden von VS oder die Nichtbeachtung des VS-NfD-Merkblattes ist unverzüglich dem oder der SiBe – soweit bestellt, alternativ der Geschäftsführung – mitzuteilen, der/die dann den VS-Auftraggeber und das BMWi (Referat ZB 3) informiert, um einen eventuell entstandenen Schaden zu begrenzen und den Vorfall aufzuklären.

4 VS-Auftrag entsteht

Wann spricht man von einem VS-Auftrag und wie entsteht ein solcher Auftrag? Das sind für ein Unternehmen spannende Fragen. Im Folgenden wird der Begriff „VS-Auftrag“ durchgängig verwendet.

Der Begriff des VS-Auftrages ist weiter gefasst als der kaufmännische Auftragsbegriff. So kann ein VS-Auftrag schon bei der Auftragsanbahnung oder Beteiligung an einer Ausschreibung bestehen, sodass alle Vorschriften für VS-NfD bereits in dieser Phase verpflichtend sind.

Grundsätzlich können öffentliche Auftraggeber VS-NfD-Aufträge an jedermann vergeben. Ein beauftragtes Unternehmen muss im Vorfeld keine speziellen Voraussetzungen erfüllen, etwa dass es sich in der Geheimschutzbetreuung des Bundes befindet. Es muss sich „lediglich“ zur Einhaltung des VS-NfD-Merkblattes [VS-NfD-MB] verpflichten und die darin beschriebenen Maßnahmen umsetzen.

In der Praxis kann es jedoch geschehen, dass bereits Teile der Ausschreibungsunterlagen VS-NfD-eingestuft sind. Schon hier ist Vorsicht geboten. Insbesondere dann, wenn die Ausschreibungsunterlagen per E-Mail oder Fax eingetroffen sind oder auf einem USB-Stick von der Vorbesprechung mitgebracht wurden, ist man bereits mitten in einem VS-NfD-Auftrag, ohne dass die nach dem VS-NfD-Merkblatt erforderlichen Maßnahmen vorher diskutiert oder gar umgesetzt wurden.

4.1 „VS-NfD ist doch harmlos“ – oder gibt es vielleicht doch Risiken?

Ist die Verschlusssache im Unternehmen, unterliegt diese sofort unterschiedlichen Auflagen – zum Teil sehr schwerwiegenden. Das beginnt mit dem Strafgesetzbuch [StGB]. Im zweiten Abschnitt „Landesverrat und Gefährdung der äußeren Sicherheit“ ist im §93 der Begriff des Staatsgeheimnisses definiert:

> *„(1) Staatsgeheimnisse sind Tatsachen, Gegenstände oder Erkenntnisse, die nur einem begrenzten Personenkreis zugänglich sind und vor einer fremden Macht geheim gehalten werden müssen, um die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland abzuwenden.“*

Die folgenden Paragrafen 94–101 definieren eine Reihe von Straftatbeständen, von *Landesverrat, Offenbaren von Staatsgeheimnissen und landesverräterische Agententätigkeit* bis hin zur *geheimdienstlichen Agententätigkeit*, die jeweils mit Freiheitsstrafen, in minderschweren Fällen mit Geldstrafen, belegt sind.

Trotz dieses massiven Strafmaßes können VS-NfD-Aufträge ohne weitere Voraussetzungen an jedermann vergeben werden. So kann leicht der Eindruck entstehen, es sei „alles halb so schlimm – VS-NfD wird schon kein Staatsgeheimnis sein“. Zur Klärung dieser Frage lohnt sich ein Blick in das Sicherheitsüberprüfungsgesetz (SÜG). §4 definiert:

> *(1) Verschlusssachen sind im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse, unabhängig von ihrer Darstellungsform. Sie werden entsprechend ihrer Schutzbedürftigkeit von einer amtlichen Stelle oder auf deren Veranlassung eingestuft.*

Das SÜG §4 (2) definiert, was VS-NfD eigentlich bedeutet:

4. VS-NUR FÜR DEN DIENSTGEBRAUCH, wenn die Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein kann.

Damit ist die Verbindung zu den Regelungen des Strafgesetzbuches hergestellt und offensichtlich: Es ist „nicht halb so schlimm", sondern schlimmer. Durch die Annahme von VS-NfD durch Mitarbeiter, die nicht entsprechend vorbereitet und verpflichtet wurden, setzen sich der Mitarbeiter und das Unternehmen enormen Risiken aus, die massive strafrechtliche Konsequenzen haben können.

Verschlusssachen dürfen nur belehrten Personen und solchen, die die Information für die Auftragsdurchführung unbedingt benötigen, gemäß dem Grundsatz 1:, „Kenntnis nur, wenn nötig", zugänglich gemacht werden. Unternehmen, die VS-NfD erhalten, müssen sicherstellen, dass jeder, der mit der Verschlusssache in Berührung kommt, *nachweislich* über den Inhalt des VS-NfD- Merkblattes des BMWi belehrt wurde (s. Kapitel 7.2). Es stellt sich also die Frage: Wer trägt im Unternehmen die Verantwortung für diesen Vorgang, wenn es keinen Sicherheitsbevollmächtigten gibt? Warum ist das wichtig? *„In Deutschland kann sich das BMWi beim VS-Auftragnehmer über die Einhaltung der Bestimmungen dieses Merkblattes vergewissern."* [VS-NfD-MB]. Für diesen Fall sollte man gerüstet sein und den Prozess VS-NfD-Belehrung sauber definiert und auditierbar umgesetzt haben.

Eine Weitergabe von VS-NfD darf nur an Regierungsstellen, zwischenstaatliche Organisationen oder Auftragnehmer erfolgen. Auch diese Anforderung erfordert einen Kontrollprozess im Unternehmen (siehe Kapitel 7) und verursacht damit Aufwände und Kosten, die bei der Bewertung, ob ein Auftrag angenommen werden kann, einfließen müssen.

Abschließend darf man nicht vergessen, dass auch für VS-NfD-Informationen eine 30-jährige Einstufung gilt. D.h., für diesen Zeitraum muss der Schutz der Information gewährleistet sein.

4.2 Weitere Fallstricke

Das VS-NfD-Merkblatt verweist an mehreren Stellen direkt oder indirekt auf nähere Festlegungen des BSI. Zu diesen Vorgaben gehören wichtige Einsatz- und Betriebsbedingungen von für VS-NfD zugelassenen Systemen sowie spezielle technische Leitlinien. Diese Unterlagen müssen bei der Planung von VS-NfD-Umgebungen mit berücksichtigt werden.

Jedoch sind diese Vorschriften vom BSI nicht allgemein verfügbar gemacht und sind teilweise sogar selbst eingestuft. Da das BSI für Geheimschutzfragen keinen Beratungsauftrag gegenüber der Wirtschaft hat, werden sie auch auf Nachfrage vom BSI nicht an Firmen abgegeben.

Für Unternehmen, die nicht in der Geheimschutzbetreuung des Bundes sind und deshalb keinen etablierten Beratungskontakt zum BMWi haben, kann es deshalb problematisch sein, an diese Vorschriften zu kommen oder überhaupt Kenntnis von deren Existenz zu erhalten. Eine Möglichkeit ist die direkte Nachfrage bei Anbietern entsprechender Lösungen, die jedoch zuvor bekannt sein müssen.

In der Konsequenz lassen sich unter Umständen nicht alle sicherheitsrelevanten Vorschriften einsehen.

Eine andere Situation, die in der Praxis durchaus vorkommen kann, ist die nachträgliche Heraufstufung von einzelnem VS-NfD-Material (z.B. Fertigungs-Unterlagen) auf „VS-Vertraulich“. Im Gegensatz zum vorher geschilderten Fall gelten in dieser Situation dann die Schutzmaßnahmen und Nachweispflichten für VS-Vertraulich für alle Kopien des ehemaligen VS-NfD-Materials. Da dieses jedoch nicht von vornherein den strengen Kontrollen für VS-Vertraulich unterlag, ist es für ein Unternehmen nur mit erheblichem Aufwand möglich, dies nachträglich, z.B. für jede Kopie und jede Kenntnisnahme, zu realisieren, wodurch das Unternehmen und die handelnden Personen großen Risiken ausgesetzt werden. Darüber hinaus erzwingt ein solcher Vorgang, dass das betroffene Unternehmen sich in den amtlichen Geheimschutz begibt.

Allerdings kann der VS-Auftraggeber Informationen nicht willkürlich einstufen. Wie dieses genau zu erfolgen hat, ist im Geheimschutzhandbuch, Kap. 6.7.1 (1) [GHB], bzw. [SÜG] geregelt.

4.3 Checkliste

- ❑ Müssen Dritte (ggf. interne Dienstleister) für die Erbringung des VS-Auftrags eingebunden werden?
- ❑ Wurde die Unterbeauftragung mit dem VS-Auftraggeber abgestimmt und sind VS-NfD-Auflagen vertraglich mit Dritten vereinbart?
- ❑ Ist ein Verantwortlicher für die Einhaltung der VS-NfD-Vorschriften definiert?
- ❑ Wurde der Verantwortliche im Unternehmen bekannt gemacht?
  Er muss immer informiert werden, wenn VS-NfD im Unternehmen verarbeitet werden soll.
- ❑ Wurden betroffene Mitarbeiter *nachweislich* gemäß VS-NfD-Merkblatt belehrt? Ist die zentrale Dokumentation sichergestellt?
- ❑ Sind technische Voraussetzungen gemäß VS-NfD-Merkblatt im Unternehmen vorhanden? Details siehe Kapitel 8.
- ❑ Gibt es im Unternehmen Regelungen für Telearbeit?
  Telearbeitsregelung gemäß VS-NfD-Merkblatt anpassen.

5 Bearbeitung des Auftrags

5.1 Betriebsmittelbereitstellung

Wurde der Auftrag schließlich erteilt, steht die Vorbereitung der Auftragsbearbeitung an, die Personal- und Betriebsmittelbereitstellung. Im Weiteren wird davon ausgegangen, dass die Bearbeitung der eingestuften Informationen mithilfe von IT erfolgt und dass die verwendeten IT-Arbeitsplatzgeräte in der Regel „tragbar“, sprich Notebooks, sind, wie es heute in der Industrie überwiegend Standard ist.

Die aktuellen Regelungen für die Verarbeitung von VS-NfD auf IT unterscheiden zwei grundsätzliche Anwendungsfälle: Einzelplatz- und vernetzte Systeme. Einzelplatzsysteme sind vollständig isolierte Geräte ohne jegliche Netzwerkfunktionen (WiFi, Bluetooth, Ethernet, ISDN ...), auf denen VS-NfD lokal bearbeitet wird. VS-NfD-Daten gelangen über Speichermedien (USB-Stick, CD-ROM, DVD, Wechselplatte, ...) auf diese Systeme. Wird ein Einzelplatzsystem mit dem Firmennetzwerk verbunden, ist zu beachten, dass sofort die Regelungen für vernetzte Systeme für das gesamte Netzwerk, an das das Einzelplatzsystem angeschlossen wurde, zu beachten sind.

Besteht die Notwendigkeit, Arbeitsgruppen mit mehreren Rechnern auszustatten und diese über ein Netzwerk miteinander zu verbinden, gelten die Anforderungen für vernetzte Systeme. Das VS-NfD-Merkblatt beschreibt in Abschnitt II die hierzu notwendigen Maßnahmen. Geräte dürfen nicht direkt ohne den Schutz durch eine Firewall, die sich entweder im Netzwerk oder auf dem Gerät befindet, mit dem Internet verbunden werden. Problematisch für Unternehmen ist die in [VS-NfD-MB, Abschnitt II 1.3] gestellte Forderung, dass nur vom BSI zugelassene Funknetzwerke verwendet werden dürfen. Dies bedeutet faktisch, dass WLAN im Unternehmen nicht im Rahmen der Bearbeitung oder Übertragung von VS-NfD genutzt werden kann, sofern keine vom BSI zugelassene Verschlüsselung eingesetzt wird. Datenträger von tragbaren Geräten, die für die Bearbeitung oder Speicherung von VS-NfD verwendet werden, müssen ebenfalls mit vom BSI zugelassenen Produkten verschlüsselt werden.

Diese Anforderungen stellen eine große Herausforderung dar, da sie eine Zulassung der verwendeten Produkte durch das BSI vorsehen. Die Anzahl der vom BSI für die Verarbeitung von VS-NfD zugelassenen Produkte ist jedoch eingeschränkt. Die möglichen Optionen reduzieren sich dramatisch, wenn man Lösungen für aktuelle Betriebssysteme oder Hardwareplattformen sucht.

Jedes IT-Gerät muss regelmäßig auf Virenbefall geprüft werden, bevor VS-NfD damit verarbeitet wird. Auf den Geräten darf sich keine private Software befinden und es dürfen keine privaten Datenträger genutzt werden.

Sind auf fest installierten Datenträgern VS-NfD im Klartext gespeichert, ist im Wartungsfall darauf zu achten, dass diese Daten sicher gelöscht werden oder der Datenträger ausgebaut und zurückgehalten wird, bevor das Gerät zur Reparatur geht. Ist dies nicht möglich und soll ein Wartungsdienstleister eingesetzt werden, ist zuerst die Weitergabezustimmung des VS-Auftraggebers einzuholen und der

Dienstleister vertraglich auf die Einhaltung des VS-NfD-Merkblattes zu verpflichten.

In Kapitel 8.2 ff. finden sich weitere Detaillierungen zu den technischen Maßnahmen.

5.1.1 Übertragung von VS-NfD

In der heutigen Zeit ist die Vernetzung von Prozessen und Geräten nicht mehr aus dem Alltag wegzudenken. Auch VS-NfD darf elektronisch übermittelt werden, wenn man bestimmte Randbedingungen berücksichtigt. Für die **Übertragung in Deutschland** ist ein BSI-zugelassenes oder vom BMI oder im Einzelfall vom BMWi freigegebenes Kryptosystem [2] notwendig. Bei grenzüberschreitender elektronischer Übermittlung müssen die Verschlüsselungsverfahren zwischen den nationalen Sicherheitsbehörden der beteiligten Staaten abgestimmt werden.

Es gibt auch Fälle, in denen ausnahmsweise eine unverschlüsselte Übertragung möglich ist:

- Bei Telefonaten oder Videokonferenzen, bei Fax oder Fernschreiben, wenn für die Übertragungsart keine Verschlüsselungsmöglichkeit besteht. Man muss sich dann vor der Übertragung davon überzeugen, dass man mit dem richtigen Empfänger verbunden ist.
- Innerhalb eines geschlossenen Netzwerkes (LAN), wenn es ausschließlich auf einem örtlich zusammenhängenden, firmeneigenen Gelände betrieben wird und es gegen unmittelbaren Zugriff Unbefugter geschützt ist.

5.1.2 Telearbeit[3]

Die Bearbeitung von VS-NfD in Privaträumen stellt eine Ausnahme dar, ist aber nach Prüfung durch den SiBe und wenn dies nicht durch den VS-Auftraggeber untersagt wurde, möglich [VS-NfD-TA]. Der Mitarbeiter muss der Kontrolle der Einhaltung der Regelungen des VS-NfD-Merkblattes in den privaten Räumen zustimmen. Ihm sollte im Vorfeld bewusst gemacht werden, dass das Unternehmen und das BMWi die Einhaltung der Regeln des VS-NfD-Merkblattes jederzeit unangekündigt überprüfen können. Eine private Nutzung der dafür verwendeten IT ist nicht erlaubt [VS-NfD-IT].

5.1.3 Kennzeichnungspflicht

VS-NfD-eingestuftes Material muss deutlich gekennzeichnet werden. Dokumente sind durch schwarzen oder blauen Stempelaufdruck „VS – NUR FÜR DEN DIENSTGEBRAUCH“ am oberen Rand einer jeden beschriebenen Seite sowie aller eingestuften Anlagen zu kennzeichnen. Bei Büchern, Broschüren u.Ä. genügt die Kennzeichnung auf dem Einband und dem Titelblatt. Kennzeichnungspflicht gilt sowohl für Dokumente wie für Geräte und Datenträger. Ist es aus Platzgründen nicht möglich, Geräte oder Datenträger direkt zu kennzeichnen, muss die Kennzeichnung am Aufbewahrungsgefäß angebracht werden.

---

[2] BSI-Schrift 7164: Liste der zugelassenen IT-Sicherheitsprodukte und -systeme [BSI – 7164]

[3] Der Begriff Telearbeit bezieht sich ausschließlich auf die „Teleheimarbeit“, s. http://de.wikipedia.org/wiki/Telearbeit

5.1.4 Aufbewahrung

VS-NfD sind in verschlossenen Räumen oder Behältern (Schränken, Schreibtischen usw.) zu verwahren. Außerhalb von solchen Räumen oder Behältnissen sind sie stets so aufzubewahren bzw. zu behandeln, dass Unbefugte keinen Zugang zur oder Einblick in die VS haben.

5.2 Realitätscheck

5.2.1 Vernetzte IT aus Sicht des VS-NfD-Merkblattes

Nun soll betrachtet werden, wie das VS-NfD-Merkblatt IT definiert. Wie immer im Geheimschutz orientiert sich das Merkblatt an der „Physik“, also den Geräten oder Übertragungswegen und daran, wo sie sich befinden. Ein „LAN“ ist als örtlich zusammenhängendes, ausschließlich auf einem abgeschlossenen Firmengelände befindliches und gegen unmittelbaren Zugriff durch Unbefugte geschütztes Netzwerk definiert. Innerhalb der Grenzen dieses „LANs“ darf unverschlüsselt übertragen werden. In allen anderen Fällen muss mit einem vom BSI, BMI oder im Einzelfall auch vom BMWi zugelassenen Produkt verschlüsselt werden [BSI - 7164].

Im Weiteren unterscheidet das Merkblatt drei unterschiedliche Anwendungsszenarien und empfiehlt, wie diese mindestens zu schützen sind.

1. ***Einzelplatz oder geschlossenes Netzwerk***

   Die Basis bildet der Vorschlag, dedizierte Einzelplatzsysteme für die Verarbeitung von VS-NfD zu verwenden, die nicht vernetzt sind. Ist eine Vernetzung notwendig, sollen die Einzelplatzrechner zu einem dedizierten Netz verbunden werden, das keine weitere Verbindung zur Außenwelt hat.

2. ***E-Mail-Anschluss nach außen***

   Die nächste Stufe ist der Anschluss des geschlossenen Netzwerkes per E-Mail an die Außenwelt. Der Netzwerkübergang muss mit einer Firewall und NAT realisiert werden. Eine Übertragung nach außen darf nur verschlüsselt erfolgen. Es dürfen nur vom BMWi zugelassene Produkte für die Verschlüsselung eingesetzt werden.

   Da in diesem Szenario nur die E-Mail-Übertragung gemeint ist, müssen VS-NfD-Daten vor der Übertragung per E-Mail verschlüsselt werden. Hierfür steht heute lediglich ein zugelassenes Produkt, das vom BSI herausgegebene CHIASMUS, zur Verfügung.

3. ***E-Mail- und Internetanschluss***

   Soll den Anwendern auch noch der Zugang zum Internet ermöglicht werden, ist zusätzlich ein Applikations-Gateway zu installieren.

5.2.2 Fazit

Das VS-NfD-Merkblatt und der dort verwendete IT-Begriff orientieren sich sehr an physischen Gegebenheiten und Anwendungsfällen. Im Geschäftsalltag gibt es jedoch viele weitere Anwendungsszenarien, beispielsweise B2B-Portale, Customer-Relationship-Management-Systeme, Auftragsbearbeitung mit ERP-Systemen, verteilte Entwicklungsumgebungen oder Systeme für

Unternehmensnetzwerke heute

Daten und IT-Geräte sind heute mobil und IT-Infrastrukturen müssen dies unterstützen, um die geforderte Produktivität zu gewährleisten. Hinzu kommt, dass mittlerweile immer mehr Dienste nicht mehr innerhalb des eigenen Unternehmens betrieben werden, sondern ausgelagert, also in der Cloud in Anspruch genommen werden. Virenschutz, Firewall und VPN-Technik sind zum technischen Standard geworden, d.h., sie befinden sich fast überall im Einsatz und man kann davon ausgehen, dass sie vorhanden sind. Auch Festplattenverschlüsselung zum Schutz der Daten ist zum festen Bestandteil moderner Betriebssysteme geworden und wird daher immer häufiger eingesetzt.

Darüber hinaus wird in Unternehmen VoIP (Voice over IP) für die Telefonie und für Videokonferenzen genutzt und damit werden bestehende ISDN-Infrastrukturen abgelöst. Kommunikation ist nicht zwingend eine bilaterale Angelegenheit mit definierten Sendern und Empfängern, sondern es geht um unterschiedliche Möglichkeiten der Kollaboration über Standorte und Zeitzonen hinweg, synchron und asynchron. Neben der E-Mail hat sich daher eine Reihe von Diensten etabliert, beispielsweise Wikis, Blogs, Team-Communities und die Techniken der sozialen Netzwerke, die auf die Nutzung im Unternehmensumfeld adaptiert werden.

Der LAN-Begriff im Unternehmen ist sicherlich in vielen Fällen anders definiert als im VS-NfD-Merkblatt, da Unternehmen nicht auf die physischen Begrenzungen eines Campus achten, sondern in Informationsdomänen denken, die dann die Schutzzonen und deren Übergänge definieren. Lokale Netzwerke (LANs) in den einzelnen Unternehmensstandorten werden häufig über VPNs miteinander verbunden, sodass sie sich dem Benutzer als ein großes Netzwerk präsentieren. Klassische Firewalls sind innerhalb des Netzwerkes daher eher selten anzutreffen und meist nur dort, wo lokale Übergänge in das Internet oder Netzwerke unterschiedlichen Schutzniveaus implementiert werden.

Geschäftsberichterstattung. Etablierte Arbeitsabläufe in Unternehmen bleiben dadurch unberücksichtigt, wodurch für Unternehmen, die das Merkblatt anwenden müssen, ein enormes Spannungsfeld entsteht.

Außerdem muss bei der Verwendung von BSI-zugelassenen Produkten die jeweilige Einsatzempfehlung der Zulassung beachtet werden. Nur unter den dort beschriebenen Bedingungen darf das Produkt verwendet werden.

Unternehmen nutzen heute häufig COTS (Commercial of the shelf)-Technik zur Absicherung ihrer IT. Diese Produkte sind jedoch maximal nach „Common Criteria“ evaluiert und zertifiziert und haben in der Regel keine Zulassung für die Verarbeitung von VS-NfD.

5.3 Checkliste

- ❑ Betreibe ich das Netzwerk auf meinem Gelände (Verfügungsgewalt) durch eigene Mitarbeiter und befinden sich alle Datenserver auf meinem Betriebsgelände?
- ❑ Kennzeichnung der Verschlusssache, Geräte und Datenträger umgesetzt?
- ❑ Firewall auf dem IT-System installiert?
- ❑ Keine Funktastatur?
- ❑ Kein Funknetzwerk?
- ❑ Datenträger mit BSI-zugelassenem Produkt verschlüsselt?
- ❑ Regelmäßige Prüfung auf Virenbefall?
- ❑ Keine private Hardware, Software oder Datenträger für VS-NfD-Bearbeitung im Einsatz?
- ❑ Löschung von Datenträgern durch mind. zweifaches Überschreiben?
- ❑ Ist das Kryptosystem für die Datenübertragung vom BSI zugelassen oder vom BMI oder im Einzelfall vom BMWi freigegeben?

- ❑ Bedingungen an die Einsatzumgebung für das zugelassene VS-NfD-Produkt erfüllt?
- ❑ Ist das LAN für VS-NfD-Bearbeitung freigegeben?
- ❑ Regelmäßige Kontrolle von Netzwerdruckern und -kopierern in zentralen Druckerräumen

6 Auftragsende

6.1 VS-Auftrag ist abgeschlossen

Mit Abschluss eines VS-NfD-Auftrags besteht die Verpflichtung zur Geheimhaltung der erhaltenen oder selbst erstellten VS-NfD weiter. Die einmal gemachte Einstufung besteht 30 Jahre fort, wenn der VS-Auftraggeber diese nicht vorher aufhebt – oder aber verlängert. Erst nach Aufhebung der Einstufung durch Zeitablauf oder durch den VS-Auftraggeber gelten die ehemaligen VS-NfD als offen.

Wenn die VS-NfD also nicht aus geschäftlichen Gründen nach Auftragsende aufbewahrt werden müssen, können Sie u.U. an den VS-Auftraggeber zurückgegeben werden. In der Praxis aber wird eine Vielzahl an VS-NfD zurückbleiben, die unter Fortbestand aller Geheimhaltungsanforderungen aufzubewahren sind, sofern sie nicht vernichtet werden dürfen. Hierzu finden sich Hinweise in Kapitel 8.5.

- Erfolgte VS-NfD-Belehrungen und andere Nachweise sollten sicher aufbewahrt werden, um auch später ggf. die Einhaltung der personellen Geheimschutzmaßnahmen belegen zu können.

7 Organisatorisches Kapitel

7.1 Verantwortlicher für Geheimhaltung

Die Verantwortung für das jeweilige Unternehmen liegt immer bei der Geschäftsführung. Wie bereits in Kapitel 4 beschrieben, kann es durchaus in der Praxis vorkommen, dass die Existenz eines VS-NfD-Auftrages im Unternehmen nicht immer bekannt ist. Das BMWi hat deshalb in der Anlage 4b [VS-NfD-IT] Formulierungen festgelegt, mit denen sichergestellt werden soll, dass bei der Auftragsannahme im Unternehmen auch gleich ein Verantwortlicher und Stellvertreter für die Einhaltung und Durchführung der VS-NfD-Maßnahmen im Unternehmen benannt wird. Bei geheimschutzbetreuten Unternehmen ist dieses automatisch der SiBe.

Die Anlage 4b definiert auch, für welche Maßnahmen der VS-NfD-Verantwortliche im Unternehmen verantwortlich sein soll. Dies umfasst neben der nachprüfbaren Belehrung und Verpflichtung der Mitarbeiter auf das VS-NfD-Merkblatt die Definition von besonderen Maßnahmen bei der Nutzung von IT, die Einholung notwendiger Genehmigungen zur Weitergabe von VS-NfD oder einer Unterbeauftragung Dritter sowie die Kontrolle der Einhaltung aller erforderlichen Maßnahmen zum Schutz von VS-NfD im Unternehmen. Das ist ein breites Spektrum an Verantwortung, das im Vorfeld einer Beauftragung im Unternehmen bekannt sein sollte.

7.2 Belehrung von Mitarbeitern

Entscheidend für das Unternehmen ist der Nachweis, dass eine Belehrung und Verpflichtung auf das VS-NfD-Merkblatt stattgefunden hat, denn durch die Anerkennung des VS-NfD-Merkblattes als Vertragsbestandteil wird gleichzeitig akzeptiert, dass sich zum Beispiel das BMWi vor Ort über die Einhaltung der Bestimmungen des Merkblattes vergewissern kann. Daher muss die Belehrung vom Unternehmen schriftlich dokumentiert werden. Ein Beispiel für eine Verpflichtungserklärung befindet sich in Kapitel 12.

Mitarbeiter, die sich im Umgang mit VS als ungeeignet erweisen oder gegen die Verpflichtung zur Geheimhaltung verstoßen haben, sind von der Bearbeitung von VS auszuschließen.

7.3 Amtliche Einstufung vs. „auf Veranlassung“

Verschlusssachen, und damit auch VS-NfD, werden aufgrund ihres Schutzbedarfs „von amtlicher Stelle“ oder „auf amtliche Veranlassung“ eingestuft.

Daraus folgt zunächst, dass nur eine Behörde die Einstufung verfügen, also den Schutzbedarf einer Information bewerten kann. Andere Informationen im Unternehmen oder im Kontext eines VS-NfD-Auftrags können einen ähnlichen Schutzbedarf haben, unterliegen jedoch ohne die staatliche Einstufung nicht den Anforderungen des VS-NfD-Merkblattes.

Das obige Zitat aus dem GHB nennt zwei Fälle einer Einstufung:

- **die amtliche Einstufung**

  Im ersten Fall bestimmt eine Behörde („amtliche Stelle“) unmittelbar, dass ein bestimmtes Dokument oder ein anderer Informationsträger als VS-NfD

eingestuft ist. In der Kennzeichnung lässt sich diese Form der Einstufung am Vermerk „amtlich eingestuft“ erkennen.

- **die Einstufung „auf amtliche Veranlassung“**

  Der zweite Fall, die Einstufung „auf amtliche Veranlassung“, kommt dann vor, wenn z.B. ein Unternehmen einen VS-NfD-Auftrag erhalten hat und der Auftrag die Weisung enthält, dass bestimmte Informationen, die das Unternehmen im Rahmen des Auftrags selbst erstellt, einzustufen sind.

  Da die Information noch nicht existiert, kann die Behörde diese nicht vorab selbst einstufen; sie weist vielmehr das Unternehmen an, dies zu erledigen. Bei Dokumenten ist eine solche Einstufung am Vermerk „auf amtliche Veranlassung eingestuft“ erkennbar.

VS-Aufträge höherer Einstufungsgrade kennen besonders für den zweiten Fall eine sogenannte Einstufungsliste, die Teil des VS-Auftrags ist und verbindlich alle Informationstypen aufführt, die einzustufen sind, und den jeweiligen Einstufungsgrad festlegt. Diese Einstufungsliste erzeugt Sicherheit und Verbindlichkeit bei der für Unternehmen schwierigen Bewertung, ob eine selbst erhobene oder erstellte Information im Kontext eines VS-Auftrags nun einzustufen ist oder nicht.

Da die Notwendigkeit der Einstufungsliste im GHB nur für VS-Aufträge oberhalb VS-NfD gefordert ist, fehlt diese in der Regel bei VS-NfD-Aufträgen. Dies kann zu Unsicherheiten bei der Einstufung führen. In der Praxis werden aus dieser Unsicherheit häufig zu viele Informationen eingestuft, wodurch sich der Aufwand zu deren Schutz erheblich erhöhen kann, da unerwartet viele Informationen nach den Regeln des VS-NfD-Merkblattes behandelt werden müssen.

7.4 VS-NfD-Belehrung

Personen, die Zugang zu VS-NfD haben oder sich verschaffen können, müssen *nachweislich* über den Inhalt des VS-NfD-Merkblattes belehrt worden sein.

Wichtig ist der Punkt *nachweislich*. Hier muss organisatorisch im Unternehmen geklärt werden, wer eine Übersicht über belehrte und auf das VS-NfD-Merkblatt verpflichtete Personen führt. Diese sollte zentral verwaltet werden, unabhängig vom jeweiligen VS-Auftrag.

Vor der Belehrung sollte klar festgestellt werden, welche Personen Zugang haben bzw. sich Zugang zu VS-NfD-eingestuften Material beschaffen können.

Hierzu sollte für jeden VS-Auftrag ein verantwortlicher Mitarbeiter (Bauleiter, Projektleiter) festgelegt werden. Dieser meldet der o.g. zentralen Funktion die Personen, die am VS-Auftrag mitwirken.

Hierzu zählen nicht nur die offensichtlich am Auftrag Mitwirkenden, sondern auch die Personen, die aufgrund ihrer Tätigkeit im Umfeld des Auftrages mitwirken und sich Zugang verschaffen können. Dazu können auch Werkschutz oder Wachdienst, Reinigungspersonal, Hausmeister, Sekretär(in) usw. zählen.

Zur eigentlichen Belehrung gehört

- die Aushändigung des VS-NfD-Merkblattes und
- die schriftliche Dokumentation (siehe Anlage) der belehrten Person, dass sie sich verpflichtet hat, die Richtlinien des Merkblattes einzuhalten. In der

Dokumentation sollte explizit auf die möglichen straf- bzw. vertragsrechtlichen Konsequenzen hingewiesen werden.

Die Belehrungsdokumentation ist dauerhaft an zentraler Stelle sowie in Kopie bei dem für den VS-Auftrag verantwortlichen Mitarbeiter aufzubewahren.

7.5 Intelligentes Telefonieren

Häufig kann über die zur Verfügung stehende Telekommunikations-Infrastruktur keine VS-NfD ausgetauscht werden, weil z.B. DECT-, Mobil- oder IP-Telefone zum Einsatz kommen.

Ein einfaches und dennoch sehr wirkungsvolles Verfahren zur Lösung dieser Herausforderung lässt sich mit „intelligentem Telefonieren“ bezeichnen.

Dazu machen sich die Teilnehmer einer Telefonkonferenz im Vorfeld bereits Gedanken, welche Informationen, die für das Gespräch relevant sind, als VS-NfD eingestuft sind. Diese Informationen werden dann vor dem Gespräch sicher verschlüsselt per E-Mail ausgetauscht.

Auf diese Weise haben alle Teilnehmer die VS-NfD bereits vor dem Gespräch vorliegen, es müssen daher im Gespräch unter Umständen keine vertraulichen Informationen ausgetauscht werden.

Darüber hinaus lassen sich einige Detailinformationen, wie zum Beispiel Listen mit Bauteilen, im Vorfeld pseudonymisieren. Dazu fertigt der Verantwortliche eine Liste mit den als VS-NfD-eingestuften Bauteilen und einen Code für jedes Bauteil an. Der Code sollte keine Rückschlüsse auf das Bauteil zulassen. Dann wird die Liste mit den Bauteilen und den entsprechenden Pseudonymen ebenfalls vor der Telefonkonferenz sicher per E-Mail verteilt. Während des Gesprächs können sich dann die Teilnehmer mithilfe der Pseudonyme über die konkreten Bauteile unterhalten, ohne dass tatsächlich vertrauliche Informationen per Telefon ausgetauscht werden müssen. Dieses Verfahren lässt sich in abgewandelter Form auch für andere Fälle einsetzen.

Das Verfahren kann aber auch an Grenzen stoßen. Dann bleibt als Alternative nur ein Vor-Ort-Termin oder eine vollständig verschlüsselte Ende-zu-Ende-Lösung.

7.6 IT zur Verwaltung von VS-NfD-Vorgängen

Wenn in Unternehmen viele Mitarbeiter sicherheitsüberprüft oder VS-NfD-belehrt sind, kann schnell ein hoher Aufwand bei der Verwaltung des Personals entstehen.

Die am Markt verfügbare Systemlösung[4] kann bei der Verwaltung mit folgenden Funktionalitäten unterstützen:

- Personal-, Firmen- und Besuchskontrollverfahren
- Elektronisches VS-Tagebuch
- VS-Aufträge und Unteraufträge
- Sperr- und Kontrollzonen von Unternehmen
- Elektronischer Datenaustausch zwischen Projekten und der Geheimschutz-Abteilung
- Templates für die VS-NfD-Belehrung/-Erklärung

[4] zur Zeit beispielsweise SeCon der Firma Nord-Tec

7.7 IT-Outsourcing und -Offshoring

Die Begriffe Outsourcing und Offshoring bezeichnen generell die Verlagerung unternehmerischer Funktionen und Prozesse entweder in Tochtergesellschaften, an fremde Unternehmen oder in das Ausland. In der Regel sind es ökonomische Gründe, die ein Unternehmen veranlassen, Outsourcing oder Offshoring zu erwägen. In der IT bedeutet Outsourcing die Fremdbeauftragung von IT-Services, z.B. den Betrieb von IT-Systemen, den Einkauf von Hotline- und Helpdesk-Leistungen, etc. Das Offshoring ist dagegen in der Regel eine Beauftragung von ausländischen Tochtergesellschaften, meist aufgrund günstigerer Lohnkosten.

Beim IT-Outsourcing von Diensten, die mit der Speicherung und Verarbeitung von VS-NfD zu tun haben, macht das BMWi sehr harte Einschränkungen. Eine Beauftragung von IT-Diensten darf nicht dazu führen, dass fremde Unternehmen oder Personen (Administratoren) Kenntnis von eingestuften Unterlagen bekommen können, ohne dass der VS-Auftraggeber dem zugestimmt hat. Dieser Umstand kann bereits dann zutreffen, wenn ein Server mit VS-NfD einem fremden Unternehmen gehört oder von diesem (remote) administriert wird, selbst wenn dieser in unternehmenseigenen Serverräumen steht.

Seitens des BMWi wird auf Basis der Vorgabe argumentiert, dass *„VS-NfD nur Personen zugänglich gemacht werden darf, die im Zusammenhang mit der Auftragsdurchführung Kenntnis erhalten dürfen“*. Diese Vorgabe schließt somit aus, dass die im Rahmen des IT-Outsourcings beauftragten Fremdunternehmen bzw. deren Personal durch eine VS-NfD-Belehrung schon juristisch hinreichend verpflichtet wären und danach eingesetzt werden könnten. Vielmehr ist stets die *Zustimmung des VS-Auftraggebers* erforderlich, auf deren Basis dann die Einhaltung des VS-NfD-Merkblattes mit dem neuen Unterauftragnehmer vertraglich vereinbart werden muss.

Bezüglich Offshoring ist die Problemstellung zwar vergleichbar, aber mit zusätzlichem Aufwand verbunden, da hier das Zugänglichmachen von VS-NfD über die Landesgrenzen (in *„nicht beteiligte Länder“*) zu beachten ist. Dies gilt sowohl bei der Weitergabe an eigene Tochterunternehmen im Ausland als auch bei der Beteiligung von externen ausländischen Partnern.

Naturgemäß sind hier die Auflagen gegenüber dem Outsourcing im Inland wiederum verschärft:

- Wie bei allen Unterauftragsvergaben ist zunächst die Genehmigung des VS-Auftraggebers einzuholen.
- Abweichend von der VS-NfD-Bearbeitung in Deutschland ist aber bei ausländischen Partnern keine Verpflichtung auf das deutsche VS-NfD-Merkblatt durchzuführen. Stattdessen ist über das BMWi (für geheimschutzbetreute Unternehmen über den BMWi-Server) zu prüfen, ob zwischen der Bundesrepublik Deutschland und dem jeweiligen Land ein bilaterales Geheimschutzabkommen besteht, über das die fremde Nation den Schutz deutscher VS im eigenen Land nach dortigem Recht zusichert. Der ausländische Partner ist dann nach den in seinem Land geltenden Rechtsvorschriften zu verpflichten. Existiert kein bilaterales Geheimschutzabkommen, muss über das BMWi eine Einzelregelung mit der zuständigen ausländischen Sicherheitsbehörde beantragt werden. In diesem Fall darf die Weitergabe erst nach abschließender Zustimmung des BMWi erfolgen.

- Werden VS-NfD elektronisch in das Ausland übertragen, muss zudem das eingesetzte Verschlüsselungsverfahren mit dem BMWi und mit der ausländischen Sicherheitsbehörde abgestimmt werden, da Kryptotechnik Ausfuhrbeschränkungen unterliegt.

Die hohen Auflagen der Verarbeitung im Ausland erfordern einen langen Vorlauf und zusätzlichen Investitionsaufwand. Dies ist bei der Überlegung, solche Partner einzusetzen, vorab zu prüfen.

8 Technisches Kapitel

Das nachfolgende Kapitel intensiviert die technischen Aspekte, insbesondere die IT-technische Betrachtung, und wendet sich damit neben dem Sicherheitsverantwortlichen oder dem Sicherheitsbevollmächtigten eines Unternehmens speziell an die IT-Verantwortlichen. Zwar wurde seitens der Autoren darauf geachtet, dem IT-Fachjargon nicht zu sehr zu verfallen, für die Beschreibung von Problemstellungen und deren Lösungsansätze wird dem Leser aber dennoch ein gewisses Maß an Kenntnissen von IT-Technik und -Prozessen abverlangt, um den Rahmen des Praxishandbuchs nicht zu sprengen.

Das folgende technische Kapitel geht von folgender Prämisse aus:

Wird eine eingestufte Information verschlüsselt, entsteht ein Binärobjekt (Chiffrat), das durch die Verschlüsselung ausreichend geschützt ist und daher selbst nicht mehr als eingestuft betrachtet werden muss und somit keine weiteren Maßnahmen zum Schutz der Vertraulichkeit erfordert*

Diese Grundannahme wird teilweise von technischen Richtlinien konterkariert, die auch für die verschlüsselten Daten weitere Schutzmaßnahmen fordern, sodass eine endlose Kette entsteht.

* siehe BSI-Zulassung von CHIASMUS [BSI-Z 201-1]

8.1 Einleitung

Bei der Umsetzung von Schutzmaßnahmen in der IT bietet das VS-NfD-Merkblatt eine gewisse Orientierung. Die vorliegende Fassung [5] hat mit der aktuellen Entwicklung der IT aber nicht Schritt gehalten. Es kann daher sinnvoll sein, sich zunächst an dem Ziel zu orientieren, ein äquivalentes Sicherheitsniveau wie bei der Verarbeitung von papierbasierten VS-NfD zu erreichen und dann die notwendigen IT-Maßnahmen Schritt für Schritt zu ergänzen.

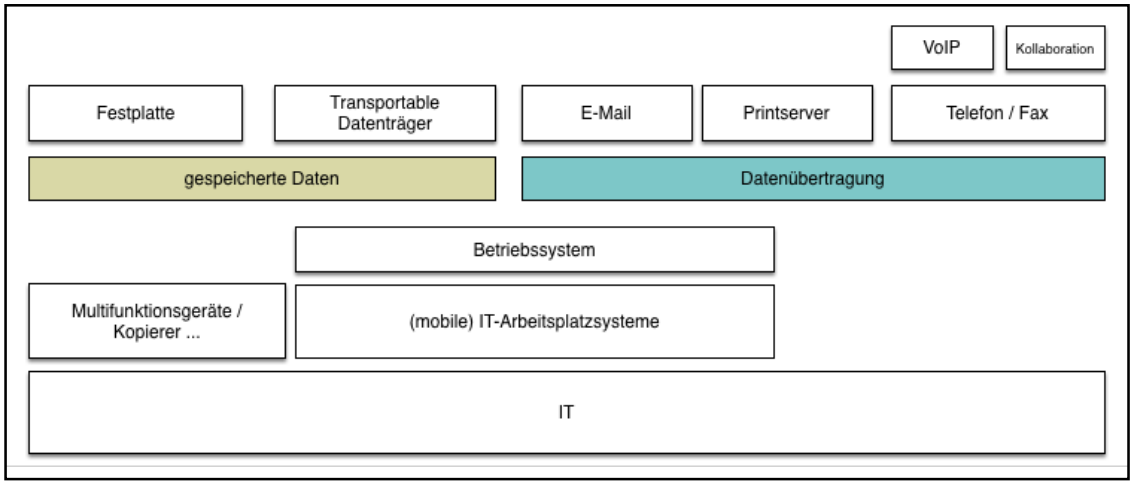

Abbildung 1: Clusterung der zu adressierenden technischen Aufgabenbereiche

Abbildung 1 beschreibt die Aufgabenbereiche, die bei der Verarbeitung von VS-NfD zu berücksichtigen sind. Sie soll dabei helfen, Teilbereiche zu behandeln und Wiederverwendbarkeit zu erleichtern. Grundsätzliche IT-Sicherheitsmaßnahmen sind heute State of the Art. Darauf bauen die folgenden Abschnitte auf, in denen zwei Benutzungsfälle („Use-Cases“) beschrieben werden:

a) verschlüsselte Verarbeitung und Speicherung sowie

b) offene Verarbeitung und Speicherung der Daten.

Vorher sollen jedoch kurz die allgemeinen Maßnahmen zusammengefasst werden.

[5] Anlage 4 des GHB vom 29. April 2014

8.2 Allgemeine IT-Maßnahmen

Generell müssen alle IT-Systeme und Datenträger, die für VS-NfD genutzt werden, in regelmäßigen Zeitabständen auf Viren und Trojaner überprüft werden [siehe VS-NfD-MB, Teil II, Absatz 1.7]. Dazu sollte auf den verarbeitenden PCs immer eine Anti-Viren-Software mit aktuellen Viren-Pattern installiert sein.

Es werden heute in der Industrie noch mehr IT-Sicherheitstechniken eingesetzt. Diese sind beispielsweise:

- Anti-Virus-Software auch auf Servern, zusätzlich häufig am E-Mail-Gateway und bei Web-Proxy, etc.
- Firewall: kontrollierte Trennung des Unternehmensnetzes von öffentlichen Netzen
- Personal Firewall: Zusätzlicher Schutz von mobilen PCs vor Angriffen aus öffentlichen Netzen
- Intrusion Detection System (IDS) / Intrusion Prevention System (IPS) / Application Control: rechtzeitige Erkennung und frühzeitige Prävention von Eindringversuchen auf die unternehmensinterne IT
- Web-Proxy: kontrollierte Nutzung von Internet-Ressourcen ohne Umgehung des Firewall-Schutzes
- Network Admission Control: kontrollierter Zugang zum internen Netzwerk
- Verschlüsselung: Festplattenverschlüsselung, VPN, SSL, E-Mail, SFTP, SCP
- Device Security → Endpoint protection / USB / Schnittstellen ...
- Netflow, Syslog, SSH ...
- Rollen- und Rechte-Management: AD, RADIUS, TACACS+, PKI ...
- Monitoring: SNMP ...
- Patchmanagement

8.3 Verschlüsselte Verarbeitung

Im Anwendungsfall „Verschlüsselte Verarbeitung“ werden die Maßnahmen zur Absicherung der Inhalte durch zugelassene bzw. empfohlene Kryptierung betrachtet. Je nach Aufgabenbereich sind verschiedene Lösungsansätze und zugelassene Produkte erforderlich.

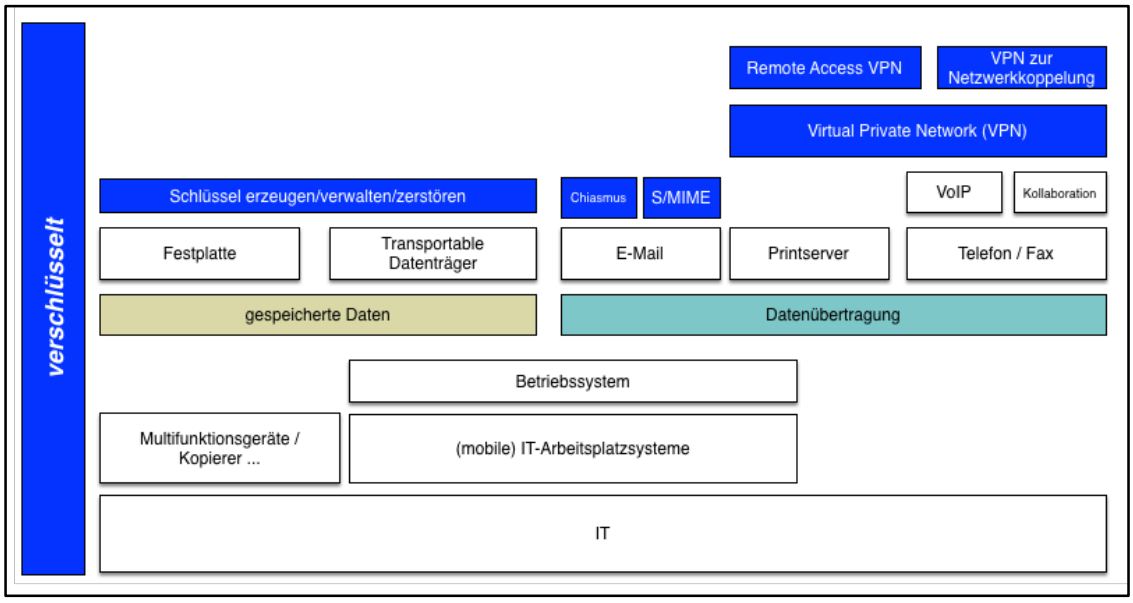

Abbildung 2: Maßnahmenblöcke bei verschlüsselter Verarbeitung

Die folgenden Kapitel betrachten die einzelnen Maßnahmenblöcke.

8.3.1 Festplattenverschlüsselung

Generell versteht man unter Festplattenverschlüsselung die vollständige Verschlüsselung eines gesamten Datenträgers bzw. einzelner Partitionen, um den unbefugten physischen Zugriff auf sensible Daten zu verhindern. Zu einem solchen Zugriff kann es beispielsweise im Fall eines Diebstahls oder versehentlichen Liegenlassens kommen. Durch die Festplattenverschlüsselung ist pauschal jedes Bit der Festplatte, egal ob es sich um das Betriebssystem, Daten oder temporäre Daten handelt, dem Zugriff entzogen. Die Verschlüsselung verhindert dabei, dass Dritte unberechtigt an die gespeicherten Daten gelangen können. Eine Festplatten(-voll-)verschlüsselung greift jedoch nur, solange das System nicht hochgefahren, also durch den Besitzer noch nicht entsperrt, wurde. Der Einsatz der Festplattenverschlüsselung ist in der Regel nur für mobile Endgeräte sinnvoll, da hier das Risiko höher liegt, dass solche Geräte entwendet werden können.

Das VS-NfD-Merkblatt[6] fordert als zwingende Schutzmaßnahme für VS-NfD den Einsatz einer BSI-zugelassenen Festplattenverschlüsselung für mobil verwendete Arbeitsplatzgeräte.

Stand Juli 2015 sind die folgenden zwei Festplattenverschlüsselungsprodukte vom BSI für Windows 7/8 zugelassen[7]:

a) TrustedDisk von der Firma Sirrix
b) SafeGuard Enterprise Device Encryption von der Firma Sophos

Zurzeit befinden sich keine weiteren Produkte in der Zulassung, weshalb die Einsatzumgebung auf Microsoft-Betriebssysteme beschränkt bleibt. Darüber hinaus empfiehlt sich ein Blick in die spezifischen Einsatzbedingungen der Produkte, an die die Zulassung geknüpft ist. Beispiel: *„Ein mit [Produkt-X] geschützter Computer darf unvernetzt oder in einem sicheren, für VS-NfD freigegebenen Netz betrieben werden*“ oder *„Ein mit [Produkt-Y] geschützter Computer darf unvernetzt oder in dem (der Organisation zugehörigen) sicheren, für VS-NfD freigegebenen Netz betrieben werden*“.

> *„Es werden folgende Anwendungsfälle unterstützt:*
> 1) *Schutz von VS an einem stationären VS-Arbeitsplatz*
>   *Sicherheitsleistung: Vertraulichkeit der VS in der Zeit, in der das System abgeschaltet ist*
> 2) *Schutz von VS an einem mobilen VS-Arbeitsplatz*
>   *Sicherheitsleistung: Vertraulichkeit der VS in der Zeit, in der das System abgeschaltet ist*
> 3) *Schutz inaktiver VS-Datenträger bei Verbringung*
> 4) *Schutz der VS bei Verlust durch Abhandenkommen / Diebstahl des ausgeschalteten Systems*
> 5) *Sicheres Löschen von Datenträgern mit VS“*

Server-Festplatten mit der oben angeführten Festplattenvollverschlüsselung zu verschlüsseln, ist wegen des dauerhaften Betriebs nicht sinnvoll. Die Produkte sind

[6] Anlage 4 vom GHB, Fassung vom 29. April 2014
[7] Der aktuelle Stand der Zulassung ist [BSI – 7164] zu entnehmen.

zudem aufgrund der interaktiven Entsperrung – d.h. es ist eine Benutzereingabe erforderlich – für eine solche Anforderung nicht anwendbar.

8.3.2 Verschlüsselte Speicherung von VS-NfD auf transportablen Datenträgern

Auf transportablen Datenträgern ist eine Verschlüsselung von VS-NfD mit den derzeit vom BSI zugelassenen Produkten zur Festplattenvollverschlüsselung nicht möglich. Im Sinne des Schutzes von VS-NfD analog zur Papierform ist jedoch eine unverschlüsselte Speicherung möglich, sofern entsprechende Aufbewahrungs- und Kennzeichnungspflichten eingehalten werden (s. Kap. 8.4.2).

Es bietet sich aber die Möglichkeit an, die Dateien auf dem transportablen Datenträger mit Chiasmus verschlüsselt abzulegen. Im Gegensatz zur vollständigen Verschlüsselung des gesamten Datenträgers wird hier nur die einzelne Datei verschlüsselt. Zum Schutz von VS-NfD ist jedoch präventiv gegen Entwendung oder versehentliches Liegenlassen eine Verschlüsselung ratsam. Um Daten sicher zu löschen, muss der transportable Datenträger mit einem geeigneten Produkt gelöscht oder vernichtet werden (siehe 8.5).

8.3.3 Verschlüsselte Übertragung

Die abgesicherte Übertragung von VS-NfD stellt einen Schwerpunkt der Arbeit für VS-NfD-Verantwortliche und deren Ansprechpartner in der IT dar.

Hier müssen zwei Anwendungsfälle unterschieden werden, die unterschiedliche Lösungen erfordern:

1. Virtual Private Networks: vollständiger Schutz des Übertragungsweges zwischen zwei Kommunikationspartnern, unabhängig von der Art des Kommunikationsprotokolls
2. Datenübertragung per E-Mail: erfordert die Verschlüsselung von eingestuften Anhängen oder den Schutz der gesamten E-Mail-Nachricht.

8.3.3.1 Virtual Private Networks (VPN)

Mit dem Begriff „Virtuelle private Netzwerke (VPNs)“ bezeichnet man verschlüsselte Punkt-zu-Punkt-Verbindungen über ein privates oder ein öffentliches Netzwerk, z.B. über das Internet. Es entsteht ein virtueller „Tunnel“, durch den die Daten sicher transportiert werden. Dabei können verschiedene Verschlüsselungs- und Authentisierungsmaßnahmen angewendet werden, um die Datenpakete zu sichern.

Es gibt in diesem Bereich mehrere Produkte, die vom BSI für VS-NfD (oder sogar höhere Geheimhaltungsstufen) zugelassen sind. Abgesehen von den hohen Preisen für solche Lösungen ist es in der Regel eine Herausforderung, derartige Spezialkomponenten in eine existierende Netzwerk-Infrastruktur eines Unternehmens zu integrieren. Daher ist dies häufig mit zusätzlichen Aufwänden verbunden (bspw. wegen spezieller Managementtools).

Bei einer VPN-Verbindung wird grundsätzlich zwischen der Verbindung entfernter Netzwerke („Netzwerkkoppelung per VPN“) und dem Fernzugang eines einzelnen Benutzers zu einem Firmennetzwerk („Remote Access per VPN“) unterschieden.

Netzwerkkoppelung per VPN

Werden Netzwerke mittels eines VPN-Tunnels miteinander verbunden, können alle Teilnehmer der beiden Netze transparent miteinander Daten über die verschlüsselte Strecke austauschen.

Es gibt verschiedene vom BSI für VS-NfD zugelassene Produkte, die in diesem Kontext verwendet werden können.

Bei größeren Standorten mit unterschiedlichen Einheiten und einer Auftragsbearbeitung im VS- sowie Nicht-VS-Umfeld ist beim Einsatz solcher Lösungen jedoch zu beachten, dass hierdurch unterschiedliche Netzverbindungen (Routing) verwaltet werden müssen und somit ein komplexeres VLAN-Management an den Standorten erforderlich werden kann.

Remote Access (RA) per VPN

Der Remote-Zugriff spielt eine immer größere Rolle in Unternehmen. Typische Einsatzszenarien sind z.B. die Störungsbehebung, aber auch moderne Arbeitsmodelle wie „Home Office“ und „Tele-Arbeit“. Mitarbeiter im mobilen Einsatz (z.B. beim Kunden oder auf Dienstreisen) profitieren von der Möglichkeit, sich sicher mit dem Unternehmensnetzwerk zu verbinden, um auf Serverdaten zugreifen zu können.

Ähnlich wie bei Netzwerkkoppelungen gibt es für diese Anforderung vom BSI für VS-NfD zugelassene Hardwarelösungen. Software-Lösungen sind dagegen vom BSI nicht zugelassen. Die Herausforderungen bei der Integration in eine bestehende Netzwerk-Infrastruktur sind denjenigen der VPN-Netzwerkkoppelung ähnlich, speziell dann, wenn es im Unternehmen bereits eine etablierte Remote-Access-Lösung ohne BSI-Zulassung gibt.

Sind die VS-NfD-Daten über mehrere Standorte verteilt, kann es notwendig werden, sowohl Netzwerkkoppelung per VPN als auch RA-VPN parallel zu betreiben.

8.3.3.2 Sichere E-Mail-Kommunikation

Arbeitsprozesse sind heute sehr stark auf die Nutzung von E-Mail angewiesen und erfordern daher eine starke Integration von Sicherheit (Verschlüsselung, Authentizität, Nichtleugbarkeit und Nachweisfähigkeit) in die benutzten E-Mail-Programme (bspw. Outlook, Lotus Notes, etc.). Sicherheitsmechanismen sollten sinnvollerweise direkt in die Prozesse integriert werden, um Bedienfehler möglichst auszuschließen.

CHIASMUS

- Benutzbarkeit: Komplexität durch viele Einzelschritte, dadurch fehleranfällig
- Limitierte Anzahl unterstützter Betriebssysteme bzw. Zulassungen
- Fehlende Integration in betriebliche Abläufe (SAP, E-Mail, Dokumentenmanagement ...)
- Fehlende Integration in Betriebssysteme (Drag-and-Drop, Ordnermanagement ...)
- Fehlendes Schlüsselmanagement, keine PKI
- Pass-Phrase muss separat verwaltet und Out-of-Band, also auf getrenntem Wege, ausgetauscht werden
- Keine Möglichkeit, Schlüssel zurückzuziehen (Revokation)
- Stellt lediglich *Vertraulichkeit* sicher (keine Authentizität, Non-Repudiation, keine Signaturen ...)
- Keine Statusinformationen über mögliche Empfänger

Für den Schutz von VS-NfD-Daten bei der Übertragung ist das Dateiverschlüsselungsprogramm CHIASMUS zurzeit die einzig zugelassene Lösung. Dies bedeutet, dass E-Mail-Anhänge vor dem Versand mit CHIASMUS lokal verschlüsselt werden müssen. Eine Integration in vorhandene E-Mail-Programme existiert nicht, daher ist dieser Vorgang manuell oder teilautomatisiert (per Scripting) vom Anwender selbst vorzunehmen.

CHIASMUS verschlüsselt nicht die E-Mail selbst, stellt also keinerlei Funktionen bereit, die die Vertraulichkeit oder Integrität der E-Mail-Kommunikation selbst betreffen. Für dieses Einsatzfeld gibt es auf Client-Seite zurzeit keine zugelassenen Produkte.

In Unternehmen haben sich hierfür S/MIME oder PGP etabliert. Hier wird ganz klar der Bereich der zugelassenen Produkte verlassen. S/MIME und PGP ermöglichen die verschlüsselte Übertragung von E-Mails und Dateien mithilfe von asymmetrischer Kryptographie und Schlüsselmanagement über weltweite Key-Server. Sie wahren damit die Authentizität, Vertraulichkeit und Integrität der gesamten E-Mail-Nachricht (ohne E-Mail-Header).

8.4 Offene Verarbeitung

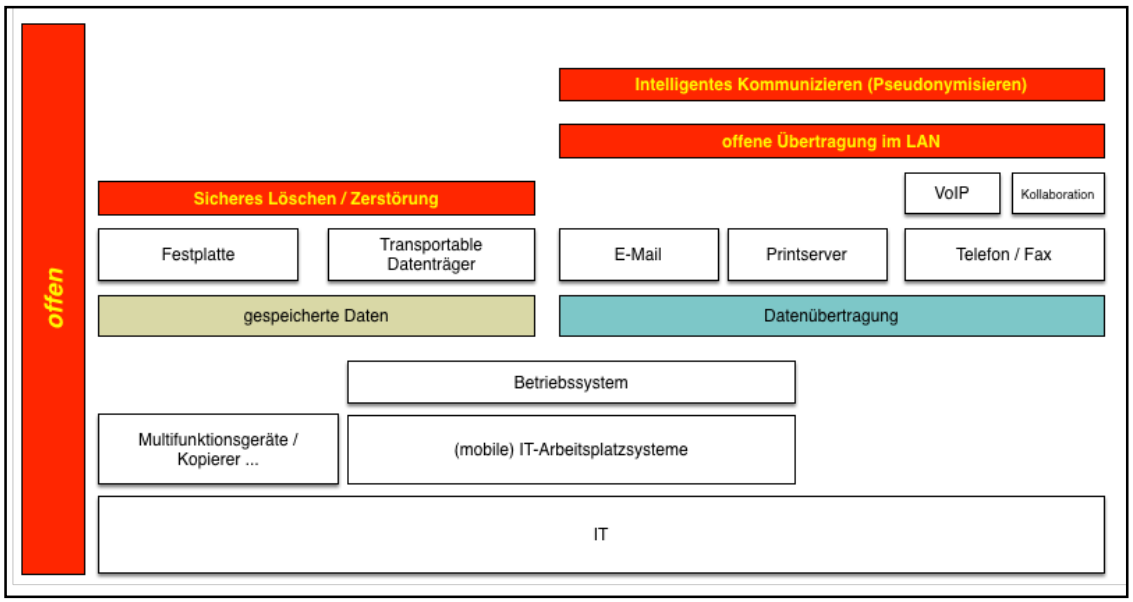

Abbildung 3: Maßnahmenblöcke bei offener Verarbeitung

8.4.1 Multifunktionsgeräte und VS-NfD

Ein Multifunktionsgerät oder auch Multifunktionsdrucker stellt heutzutage typischerweise eine Kombination der Funktionen Drucken, Scannen, Kopieren und Faxen zur Verfügung. Oft kommen in den Multifunktionsgeräten lokale Speichermedien (z.B. Festplatten) zum Einsatz. Da jeder Druck- oder Kopiervorgang temporäre Dateien der Druckdaten auf den eingebauten Speichermedien hinterlässt, müssen hierbei Sicherheitskonzepte berücksichtigt werden.

Die erweiterten Funktionen der Geräte, beispielsweise Scan-to-Mail, stellen jedoch ein Sicherheitsproblem dar, da die E-Mails oft unverschlüsselt übertragen werden.

Wenn Fachbereiche gemeinsam mit der IT-Abteilung vor der Entscheidung stehen, ob solche Multifunktionsgeräte auch für Mitarbeiter mit Umgang mit VS-NfD eingeführt werden können, sollten sie sich näher mit der vom BSI herausgegebenen technischen Richtlinie [BSI-TL-03420] beschäftigen. Weiterhin gilt natürlich auch der Rahmen, der vom VS-NfD-Merkblatt vorgegeben wird.

Die folgenden Punkte gilt es insbesondere zu berücksichtigen:

1. Für Multifunktionsgeräte wird eine „Common Criteria“[8]-Zertifizierung mit EAL 3[9] oder höher gefordert [siehe BSI-TL-03420, Abschnitt 4.3]. Eine Übersicht solcher Produkte befinden sich unter anderem auf www.commoncriteriaportal.org/products in der Kategorie „Multi-Function Devices“. Unternehmen sollten sich überzeugen, dass der EAL Level der Geräte ausreichend hoch ist und die im Security Target gemachten Annahmen mit der Einsatzumgebung in Einklang stehen. Außerdem sollte

[8] Die Common Criteria (CC) sind ein internationaler Standard für die Kriterien zur Bewertung und Zertifizierung der Sicherheit von IT-Produkten im Hinblick auf Datensicherheit, siehe auch http://www.bsi.bund.de

[9] EAL steht innerhalb der Common Criteria für „Evaluation Assurance Level“ und repräsentiert eine von sieben möglichen Stufen der Vertrauenswürdigkeit.

im Security Target geprüft werden, ob die benötigten Sicherheitsfunktionen im Produkt implementiert sind.

2. Für den Betrieb im lokalen LAN müssen die Multifunktionsgeräte in die IT-Sicherheitsmaßnahmen im Netzwerk und die organisatorischen Maßnahmen zum Schutz der VS-NfD-Daten eingebunden sein [siehe BSI-TL-03420, Abschnitt 4.3].
3. Beim Austausch bzw. der Reparatur von Multifunktionsgeräten ist insbesondere auf den sorgsamen Umgang mit Festplatten zu achten. Diese können zum Teil noch Restinformationen enthalten und müssen daher effektiv gelöscht werden. Hinweise dazu liefert wiederum [BSI-TL-03420, Abschnitt 4.3].

Daher sollte bei Leasingverträgen für Multifunktionsgeräte darauf geachtet werden, dass die Verträge so gestaltet sind, dass die in den Geräten verbauten Festplatten bei Rückgabe oder Wartung immer im eigenen Unternehmen verbleiben.

Alternativ können Unternehmen auch erwägen, für Mitarbeiter mit VS-NfD-Umgang Einzelplatzdrucker (bzw. Scanner, Kopierer oder Faxgeräte) ohne Festplatte zu beschaffen, da diese deutlich einfacher zu handhaben sind. Für die normalen Aufgaben des Mitarbeiters außerhalb der Bearbeitung von VS-NfD kann dann auch ein Multifunktionsgerät genutzt werden.

8.4.2 Offene Speicherung von VS-NfD auf transportablen Datenträgern

Die transportablen Datenträger dürfen gemäß [VS-NfD-MB, Abschnitt 1.5] VS-NfD-eingestufte Daten unkryptiert, also unverschlüsselt, enthalten. Die Datenträger sind dann jedoch gemäß Teil I 2.1.2 zu kennzeichnen[10] und gemäß [VS-NfD-MB, Teil I 2.1.3] aufzubewahren.

Dazu gehört auch, dass die VS-NfD in digitaler Form analog zur Papierform in verschlossenen Räumen oder Behältern (Schränken, Schreibtischen usw.) zu verwahren ist. Außerhalb von solchen Räumen oder Behältnissen ist die VS-NfD stets so aufzubewahren bzw. zu behandeln, dass Unbefugte keinen Zugang zu oder Einblick in die VS-NfD haben [VS-NfD-MB, Teil II, Absatz 2.1.4].

Das Gerät, mit dem die auf dem Datenträger gespeicherten Daten verarbeitet werden, unterliegt dabei den Auflagen gemäß [VS-NfD-MB, Teil II (s. auch 8.3.1)].

Um Daten sicher zu löschen, muss der Datenträger mit einem geeigneten Produkt gelöscht werden (siehe 8.5).

8.4.3 Offene Übertragung

In einem LAN, das auf einem örtlichen zusammenhängenden firmeneigenen Areal betrieben wird, ist die Übertragung von VS-NfD-Informationen unverschlüsselt möglich. Die IT-Infrastruktur muss dabei vor Zugriff durch unberechtigte Personen (firmeneigene oder Dritte) geschützt sein.

[10] Die Kennzeichnung von VS-NfD wird auch in den vom BMWi angebotenen Seminaren zum Geheimschutz näher erläutert.

8.4.4 Telefonie

Bei Gesprächen über Telefonverbindungen, unabhängig von der genutzten Technologie, kann man heute davon ausgehen, dass diese Verbindung nicht Ende-zu-Ende-verschlüsselt ist. Daher sollten die in Kapitel 7.5 beschriebenen Grundsätze berücksichtigt werden.

VS-NfD-Sachverhalte lassen sich ausnahmsweise über Festnetzverbindungen, beispielsweise ISDN oder Analog-Telefonie, besprechen bzw. per Fax übertragen, wenn der Auftraggeber dem bei der Auftragsvergabe nicht ausdrücklich widersprochen hat.

8.4.4.1 Telefon-Konferenzen

Für Telefonkonferenzen gelten grundsätzlich alle Punkte, die für Telefonie gültig sind. Die Risiken erhöhen sich jedoch durch das Vorhandensein eines Telefonkonferenz-Diensteanbieters verschärft, da dieser im Zweifel die Kommunikation mitschneiden kann.

Daher sollte man die in Abschnitt 7.5 beschriebenen Grundsätze berücksichtigen.

8.4.5 Collaboration- und Conferencing-Tools

Bei Teambesprechungen, Schulungen oder einer themenbezogenen Zusammenarbeit werden zunehmend elektronische Collaboration- bzw. (Web-) Conferencing-Tools verwendet, insbesondere bei standort- oder unternehmens-übergreifenden Konferenzen. Vorteile der Online-Konferenzen sind u.a. die Vermeidung von Reisezeiten und Reisekosten, aber auch die Möglichkeit der Aufzeichnung, z.B. einer Schulung, für eine spätere Veröffentlichung oder Auswertung.

Conferencing-Systeme bieten darüber hinaus Funktionalitäten wie

- Freigabe von Bildschirmen (Desktop) oder einzelnen Anwendungen
- File-Sharing
- Übertragung von Maus- und Tastaturkontrolle an andere Teilnehmer (s. hierzu auch Kapitel 8.7 „Remote-Steuerung/Fernwartung von IT-Systemen“)
- Whiteboard
- Chat
- Video und VoIP-Audio
- integrierte Telefonkonferenz-Funktionen u.v.m.

Die meisten am Markt verfügbaren Produkte nutzen als Implementierungsvariante das Software-as-a-Service (SaaS)-Modell. Wenige Produkte sind auch als lokale Installationen erhältlich. Diese bilden aber aufgrund des IT-Infrastrukturaufwands und der damit verbundenen Kosten vorwiegend eine Option für größere mittelständische Firmen oder Großunternehmen.

Im Zusammenhang mit VS-NfD muss jedoch die Implementierungsvariante Software-as-a-Service wegen des damit meist verbundenen Kontrollverlusts als kritisch erachtet werden. Aufgrund der eingesetzten Konferenz-Zentralen (Multi-Conference-Units – MCU) der Provider unterstützen die Produkte zwar i.d.R. eine verschlüsselte Übertragung, innerhalb der Konferenz-Zentralen ist diese Verschlüsselung aber aufgehoben. Bietet das jeweilige Produkt keine Möglichkeit, bei der elektronischen Besprechung/Präsentation von eingestuften Informationen

oder Unterlagen eine direkte Verbindung [11] zwischen den Teilnehmern aufzubauen, ist gemäß dem Prinzip „Kenntnis nur, wenn nötig“ von der Lösung Abstand zu nehmen. Möglich ist aber, die zu besprechenden Unterlagen vorab zu versenden. Zusätzlich gelten die im VS-NfD-Merkblatt aufgeführten Maßnahmen für „Telekommunikationsverbindungen“ [VS-NfD-MB, Teil II, Kap. 2.1], speziell dass sich die „absendende Stelle […] vor der Übertragung zu vergewissern [hat], dass sie mit dem richtigen Empfänger verbunden ist“.

Generell können Collaboration-/Conferencingtools *problemlos* eingesetzt werden, wenn diese als unternehmensinterne Implementierungsvariante oder in einer Punkt-zu-Punkt-Konferenz laufen und die standortübergreifende Kommunikation gemäß VS-NfD-Merkblatt verschlüsselt wird. D.h., diese Lösungen sind nicht geeignet, um mit externen Teilnehmern, beispielsweise außerhalb der firmeneigenen Telefonanlage, sicher zu kommunizieren.

8.5 Sicheres Löschen von Datenträgern

Datenträger, auf denen VS-NfD gespeichert wurden, müssen vor einer Rück- oder Weitergabe an Dritte oder vor anderweitiger Verwendung innerhalb des Unternehmens so gelöscht werden, dass die Daten nicht mehr rekonstruiert werden können.

Das VS-NfD-Merkblatt fordert deshalb, dass die Datenträger mindestens zweifach überschrieben werden, möglichst mit einem vom BSI empfohlenen Produkt: [BSI-TL-03400] und [BSI–TL-03420]. Auch wenn die Datenträger im Betrieb verschlüsselt waren, müssen sie bei einer Aussonderung oder vor Weiterverwendung außerhalb eines VS-NfD-Bereichs überschrieben werden.

Festplatten als Datenträger können in der Praxis mithilfe des vom BSI empfohlenen Open-Source-Programms DBAN[12] sicher gelöscht werden, wenn man die Grenzen des Programms beachtet. Das BSI hat hierzu ein Merkblatt mit Benutzungshinweisen zu DBAN herausgegeben.[13]

Aufgrund der Vielzahl in der Praxis vorkommender Festplattentechniken ist „sicheres Löschen“ dennoch zu einer komplizierten Angelegenheit geworden, da die Festplattensteuerungen teilweise einen direkten Zugriff auf den Datenträger verhindern und man sich deshalb nicht sicher sein kann, dass auch wirklich alle Bereiche der Festplatte überschrieben wurden. Dies gilt insbesondere für flashspeicherbasierte Systeme wie USB-Sticks und SSDs, die nicht sicher überschrieben werden können und sich deshalb nur durch Vernichtung sicher entsorgen lassen.

In jedem Fall nimmt das Überschreiben, verbunden mit der Führung eines entsprechenden Nachweises zur eigenen Absicherung, bei heutigen Datenträgergrößen erhebliche Zeit in Anspruch. Dies kann bei großen Stückzahlen (z.B. beim Austausch von Server- oder SAN-Platten) erhebliche betriebliche Aufwände bedeuten, die den Wert der Datenträger möglicherweise übersteigen.

[11] Kein Zwischenspeichern oder weitere Eingriffsmöglichkeiten in die Konferenz durch den Provider

[12] Darik’s Boot and Nuke http://www.dban.org

[13] Das BSI gibt selbst keine Löschsoftware heraus und hat über die Empfehlung von DBAN hinaus auch keine Zulassung für Löschsoftware erteilt. Das vor Jahren vom BSI selbst vertriebene Programm „VS-Clean“ ist wegen vollständiger Inkompatibilität mit aktuellen Festplatten und Controllern vom BSI zurückgezogen worden und darf nicht mehr eingesetzt werden.

Eine Alternative kann in diesem Fall die Vernichtung der Datenträger durch Zerkleinern oder Verbrennen sein.

Gleiches gilt für Magnetbänder, die heute oft in großen Stückzahlen in automatisierten Bandrobotern eingesetzt werden. Auch Bandkassetten müssen vor Weiterverwendung außerhalb eines VS-NfD-Bereichs vollständig überschrieben werden. Dieses vollständige Überschreiben erfordert viele Stunden Zeit, in der die typischerweise ständig genutzten Bandlaufwerke für andere Aufgaben blockiert sind. Auch hier ist die Vernichtung der Bänder eine mögliche Alternative.

Die Vernichtung von Datenträgern (Festplatten oder Bänder) kann durch Entmagnetisierung („Degaussen"), mechanisch (durch Zerkleinern, „Schreddern") oder thermisch durch Verbrennen bzw. Einschmelzen erfolgen. Auch hierzu macht das BSI in den oben genannten technischen Leitlinien verfahrensspezifische Vorgaben.

Wenn zur Vernichtung ein Dienstleister beauftragt wird, muss die Begleitung des gesamten Vernichtungsprozesses durch einen VS-NfD-belehrten Angehörigen des eigenen Unternehmens sichergestellt sein.

8.6 VS-NfD und aktuelle Betriebssysteme

Ein häufig anzutreffendes Problem im Umgang mit VS-NfD ist die nicht ausreichende Unterstützung von aktuellen Versionen der üblichen Betriebssysteme durch zugelassene Produkte. So wird zurzeit keines der Apple- oder Google-Betriebssysteme unterstützt. Dies stellt für einige Unternehmen ein Problem dar, da es für VS-NfD-Aufträge u.U. neue Ausstattung, Infrastruktur und Prozesse anschaffen bzw. etablieren muss. Gerade in größeren Unternehmen ist dies sehr problematisch, weil Software durch etablierte Prozesse mit langen Roll-out-Zyklen eingeführt werden muss. Ein kompletter Produktwechsel erfordert sehr viel Zeit und Geld, weil i.d.R. die im Hintergrund laufenden Supportprozesse und das Management angepasst werden müssen. Die grundsätzliche Anforderung, nur „BSI-zugelassene Produkte" zu verwenden, hat somit erhebliche Auswirkungen auf die Wirtschaftlichkeitsbetrachtung bei der Angebotserstellung.

Eine pauschale Lösung kann hier nicht angeboten werden. Folgende Punkte sollten betroffene Unternehmen jedoch in Erwägung ziehen:

- Rücksprache halten mit den Herstellern. Oft erfährt man auf diese Weise, ob sich ein aktuelles Produkt gerade in der Zulassung befindet.
- Nach Rücksprache und Klärung mit dem VS-Auftraggeber kann ggf. beim BMWi die Freigabe eines nicht oder noch nicht zugelassenen Produktes für ein spezielles Projekt erreicht werden. Auch das BSI spricht teilweise vorläufige Zulassungen für Produkte aus, welche jedoch in der Regel auf einzelne Bedarfsträger eingeschränkt sind.
- Vor der Umstellung auf neue Betriebssysteme mit der IT-Abteilung klären, ob für einzelne Projekte die Bereitstellung und Betrieb von Notebooks mit älteren Betriebssystemenversionen möglich bleibt. Für diese gibt es in der Regel zugelassene Produkte.

8.7 Remote-Steuerung/Fernwartung von IT-Systemen

Unter Remote-Steuerung oder Fernwartung versteht man Remote Access VPN-Zugriffe auf IT-Systeme von einem beliebigen Ort aus, beispielsweise über das

Internet. Zwar ist prinzipiell auch eine Remote-Steuerung von Endgeräten wie Laptops oder PCs möglich, dieser Fall ist hier jedoch nicht gemeint. Dieses Handbuch konzentriert sich auf komplexere IT-Systeme (Server, Netzwerke ...), die zwingend einen Systemzugriff durch den Hersteller oder einen IT-Dienstleister erfordern.

Zur Störungsbehebung werden zunehmend auch Mitarbeiter von externen Firmen eingesetzt, da diese über die entsprechenden technischen Kenntnisse verfügen. Müssen sie auch auf VS-NfD zugreifen, gelten hier die weiteren Rahmenbedingungen. Die dazugehörige Unterbeauftragung muss mit dem VS-Auftraggeber abgestimmt werden. Zusätzlich müssen die VS-NfD-Auflagen mit dem externen Dienstleister vertraglich vereinbart werden (z.B. Stellung von VS-NfD-belehrtem Personal, Umsetzung von „Kenntnis nur, wenn nötig“, etc.).

Es empfiehlt sich daher insgesamt, den Remote-Zugriff auf VS-NfD-Systeme zu minimieren oder ganz darauf zu verzichten. Dies lässt sich z.B. durch kombinierte technische und organisatorische Maßnahmen erreichen, bei denen eine Separierung von normalen Daten und VS-NfD in den IT-Systemen vorgenommen wird. Dann ist der Remote-Zugriff auf die normalen Daten weiter möglich, bei Zugriff auf VS-NfD muss dagegen eine herkömmliche Form der Bearbeitung erfolgen, der Techniker muss also zur Störungsbehebung an den jeweiligen Standort fahren. Da die Informationen bei einer Remote-Access-Verbindung möglicherweise das LAN verlassen, müssen diese Verbindungen mit einem vom BSI zugelassenen Kryptosystem verschlüsselt werden.

Ein Zugriff, bei dem die Daten Deutschland verlassen, ist mit zusätzlichen Auflagen verbunden (siehe VS-NfD-Merkblatt), welche u.U. zum Ausschluss führen.

Im Bereich der Fernwartung kann man sich durch weitere organisatorische Maßnahmen absichern, beispielsweise jeden Vorgang bewusst im Vier-Augen-Prinzip zu starten und zu beenden, um Missbrauch zu verhindern. Alternativ können Fernwartungszugänge mit One-Time-Password-Systemen gesichert werden, die nur einen einmaligen Zugang ermöglichen und nicht wiederverwendet werden können. Zusätzlich sind Maßnahmen auf der Netzwerkebene möglich, um den Zugriff auf einen möglichst kleinen, streng festgelegten Bereich des Netzwerkes einzuschränken.

8.8 Virtualisierung

Unter dem Begriff Virtualisierung wird in der Informatik die mehrfache Nutzung von physischen Ressourcen, beispielsweise einer CPU, eines Speichers oder anderer, durch Emulierung – d.h. Schaffung mehrerer virtueller Einheiten, die gemeinsam die zugrunde liegende physische Ressource nutzen – verstanden.

Die aktuelle Version des VS-NfD-Merkblattes macht keine Aussagen zum Thema Virtualisierung. Grundsätzlich sollte daher der Ansatz verfolgt werden, die virtuelle Umgebung genauso abzusichern, wie es eine entsprechende reale Umgebung erfordern würde, d.h.: Rechte- und Rollenkonzept, Benutzerverwaltung, Datensicherung, Redundanz, Patchmanagement, Schutz gegen Angriffe aus dem Netz, Virenschutz, etc. Darüber hinaus gibt es spezielle Sicherheitstechnik für das Rechenzentrum und für virtuelle Umgebungen, wie beispielsweise eine Studie in Zusammenarbeit mit dem BSI [BSI-vmware-EMC- Cisco] zeigt.

Virtualisierung kann zur Verbesserung der Sicherheit beitragen, da sie durch die Schaffung von „Compartments“ direkt das „Need-to-know“-Prinzip unterstützt. In

diesem Umfeld ist in Zukunft mit weiteren Lösungen und auch entsprechenden Regelungen zu rechnen, daher wird dieser Abschnitt in Zukunft weiter ausgebaut.

8.9 Cloud

Hinter dem Begriff „Cloud“ oder „Cloud Computing“ steckt ebenfalls eine Form der Virtualisierung. Cloud umschreibt den Ansatz, abstrahierte Infrastrukturen dynamisch, d.h. an den aktuellen Bedarf angepasst, über das Netzwerk zur Verfügung zu stellen. Man unterscheidet verschiedene Servicemodelle:

- **IaaS** – Infrastructure as a Service – die Bereitstellung von virtualisierten Ressourcen wie Rechnern, Netzwerken oder Speichern
- **PaaS** – Platform as a Service – die Bereitstellung von Programmierungs- oder Laufzeitumgebungen mit dynamisch anpassbaren Rechen- oder Datenkapazitäten
- **SaaS** – Software as a Service – die Bereitstellung von Software-Sammlungen und Anwendungsprogrammen

Cloud-Dienste werden in unterschiedlichen Versionen am Markt angeboten:

- Public Cloud
- Private Cloud
- Hybrid Cloud
- Community Cloud

Solange es keine verbindlichen Aussagen zur Eingangsfrage dieses Kapitels gibt, also ob verschlüsselte Objekte als nicht mehr eingestuft betrachtet werden können und damit keinen weiteren Sicherheitsmaßnahmen unterliegen, dürfen nur Private-Cloud-Ansätze (eigene Soft-/Hardware, selbst betrieben, auf eigenem Gelände), unter Berücksichtigung aller Anforderungen dieses Handbuchs, für VS-NfD-Bearbeitung eingesetzt werden.

9 Schlussbemerkung

Das Autorenteam hat versucht, Erfahrungen aus langjähriger Praxis im Geheimschutz und angewandter IT-Sicherheit in diesem Dokument zu bündeln. Der Rahmen für die Auslegung war dabei immer strikt das VS-NfD-Merkblatt des BMWi.

Einflussgrößen wie das kürzlich verabschiedete IT-Sicherheitsgesetz und das generell wachsende Sicherheitsinteresse der Behörden werden dazu führen, dass Regelungen und technische Lösungen adaptiert werden, ebenso wie dieses Dokument.

Das vorliegende Handbuch sollte als „lebendes Dokument" verstanden werden, das von den eingebrachten Praxiserfahrungen lebt. Kommentare, Anmerkungen und insbesondere Ergänzungen zu Themenbereichen, die eventuell fehlen, sind sehr gerne erwünscht. Bitte kontaktieren Sie in diesem Fall das Autorenteam unter autoren@vs-nfd-handbuch.de.

9.1 Autorenteam

9.1.1 Koordination

Klaus Lenssen	Cisco Systems GmbH

9.1.2 Autoren

Jürgen Entchelmeier	Limbach Secure Sicherheitstechnik GmbH
Oliver Gambero	IBM Deutschland GmbH
Wilfried Gericke	ehemals Fraunhofer INT
Thorsten Kammer	BWI Informationstechnik GmbH
Christian Kerckhoff	Siemens AG
Klaus Lenssen	Cisco Systems GmbH
Ralf Lubberich	IBM Deutschland GmbH
Thomas Königshofen	Deutsche Telekom AG
Sven Oliver Mende	Deutsche Telekom AG
Frank Sander	IABG mbH
Guido Scherpenstein	Fujitsu Technology Solutions GmbH
Ronald Steinbeck	Vodafone GmbH

Wir danken den vielen Kollegen aus den Länder-Arbeitskreisen der Sicherheitsbevollmächtigten, sowie den Mitgliedern des Bundesarbeitskreises der Sicherheitsbevollmächtigten (BAK SiBe), für Ihre wertvollen Anregungen und Diskussion während der Entstehung dieses Handbuches.

10 Abkürzungen

AD	Active Directory
BMWi	Bundesministerium für Wirtschaft und Energie
BSI	Bundesamt für Sicherheit in der Informationstechnik
BMI	Bundesministerium des Inneren
B2B	Business to Business
CC	Common Criteria
COTS	Commercial Of The Shelf
CPU	Central Processing Unit
DECT	Digital Enhanced Cordless Telecommunications
EAL	Evaluation Assurance Level
ERP	Enterprise-Resource-Planning
GHB	Geheimschutzhandbuch (Handbuch für den Geheimschutz in der Wirtschaft ((BMWi))
IaaS	Infrastructure as a Service
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
ISDN	Integrated Services Digital Network
LAN	Local Area Network
MB	Merkblatt
PaaS	Platform as a Service
PGP	Pretty Good Privacy
PKI	Public-Key-Infrastructure
RA	Remote Access
SAN-Platte	Storage Array Network-Platte
SaaS	Software as a Service
SCP	Secure Copy (Protokoll setzt auf SSH auf)
SFTP	Secure File Transfer Protocol
SiBe	Sicherheitsbevollmächtigte(r)
S/MIME	Secure/ Multipurpose Internet Mail Extensions
SNMP	Simple Network Management Protokol
SSD	Solid State Disk
SSH	Secure Shell
SSL	Secure Sockets Layer
SÜG	Sicherheitsüberprüfungsgesetz
TCP	Transport Control Protocol
TL	Technische Leitlinie

TLS	Transport Layer Security
USB	Universal Serial Bus
VoIP	Voice over IP
VPN	Virtual Private Network
VS	Verschlusssache
VS-NfD	Verschlusssache - Nur für den Dienstgebrauch
WLAN	Wireless LAN

11 Bibliografie

11.1 Literatur

BDSG	Bundesdatenschutzgesetz (14. August 2009)
VSA	Allgemeine Verwaltungsvorschrift des Bundesministeriums des Inneren zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA). *VS-Anweisungen – VSA*. (26. April 2010)
VS-NfD-MB	Merkblatt für die Behandlung von Verschlusssachen (VS) des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD). *VS-NfD Merkblatt (Anlage 4 GHB)*
VS-NfD-TA	Anlage 4a – Telearbeit (2. September 2008). Anlage 4a – Anlage zum VS-NfD-Merkblatt zur Behandlung von Verschlusssachen (VS) des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD) in privaten Räumlichkeiten (Telearbeit)
VS-NfD-IT	Anlage 4b (23. April 2013). Anlage zum VS-NfD-Merkblatt zur Behandlung von Verschlusssachen (VS) des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD), Vertragsbestandteil zwischen Auftraggeber und Auftragnehmer bei Verträgen mit Unternehmen bzw. sämtlichen Nachunternehmen
GHB	Handbuch für den Geheimschutz in der Wirtschaft (29. April 2014)
BSI – 7164	BSI-Schrift 7164: Liste der zugelassenen IT-Sicherheitsprodukte und -systeme
BSI – TL-03400	Produkte für die materielle Sicherheit (Juni 2013)
BSI – TL-03420	Leitlinien für das Löschen und Vernichten von schutzbedürftigen Informationen auf Datenträgern (Juni 2013)
BSI – TR-02102	Kryptografische Verfahren: Empfehlungen und Schlüssellängen (9. Januar 2013)
SÜG	*Sicherheitsüberprüfungsgesetz:* Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes (7. Dezember 2011)
StGB	Strafgesetzbuch (23. April 2014)

11.2 Downloadmöglichkeiten

BSI – 7164	https://www.bsi.bund.de/DE/Themen/Sicherheitsberatung/ZugelasseneProdukte/Liste_Produkte/Liste_Produkte_html.html
SÜG – Sicherheitsüber-prüfungsgesetz	http://www.gesetze-im-internet.de/s_g/
StGB – Strafgesetzbuch	http://www.gesetze-im-internet.de/stgb/
BDSG – Bundesdatenschutz-gesetz	http://www.gesetze-im-internet.de/bdsg_1990/
BMWi – GHB, Geheimschutz-handbuch	https://bmwi-sicherheitsforum.de/handbuch/367,0,0,1,0.html?fk_menu=0
BMWi – VS-NfD-Merkblatt	https://bmwi-sicherheitsforum.de/anlage/5/

12 Beispiel einer Mitarbeiter-Verpflichtungserklärung

[Firmenlogo]

Name: Vorname:
Geburtstag: Funktion:

VERPFLICHTUNGSERKLÄRUNG

Sie arbeiten in einem Unternehmen mit schützenswerten Informationen, die für die Bundesrepublik Deutschland von besonderer Bedeutung sind und daher eingestuft wurden.

Hiermit erkläre ich, dass ich das

Merkblatt für die Behandlung von
Verschlusssachen (VS) des Geheimhaltungsgrades
VS - NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)
Anlage zum VS-NfD-Merkblatt zur Behandlung von Verschlusssachen (VS) des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH in privaten Räumlichkeiten (Telearbeit)
[ggf. Firmenrichtlinie hinzufügen]

Grund der Verpflichtung:

[ ] Allgemeine Bearbeitung von / Zugang zu VS-NfD
[ ] VS-NfD-Projekt [Nr]:

erhalten und zur Kenntnis genommen habe und dass ich mich an die dort aufgeführten Bestimmungen halten werde.

Mir ist bekannt, dass ich für die korrekte Behandlung der mir zugänglich gemachten VS-NfD-eingestuften Verschlusssachen eine besondere und persönliche Verantwortung trage. Verstöße gegen die im Merkblatt aufgeführten Regelungen können straf-, arbeits- und/oder vertragsrechtliche Konsequenzen haben.

Auf die strafrechtlichen Konsequenzen, die sich im Fall eines Geheimnisverrats – insbesondere gemäß den §§ 93 bis 99 und 353b Abs. 2 StGB – ergeben, wurde in der Verpflichtung hingewiesen.

Der Inhalt dieser Erklärung wird von dem / der Verpflichteten anerkannt.

[Ort, Datum], den