



Mobile Datenträger

ANWENDUNG:

Empfehlungen zum Umgang mit mobilen
Datenträgern

VERSION:

1.2

DATUM:

23. Februar 2010



DVZ Datenverarbeitungszentrum
Mecklenburg-Vorpommern GmbH

Informationssicherheit ist ein Prozess und kein Produkt.

**Und wie eine Kette ist Informationssicherheit nur so stark
wie ihr schwächstes Glied.**

Die Inhalte der verwendeten Informationen aus den IT Grundschatzkatalogen im vorliegenden Dokument unterliegen dem Copyright des Bundesamtes für Sicherheit in der Informationstechnik.

Das vorliegende Dokument kann von den Internetseiten der DVZ M-V GmbH heruntergeladen und gedruckt werden. Inhaltliche Änderungen bzw. Ergänzungen sind mit der DVZ M-V GmbH abzustimmen. Eine Weitergabe ist ebenfalls mit der DVZ M-V GmbH, Bereich Marketing, abzustimmen.

Wird im Text die männliche Form verwendet, geschieht dies ausschließlich aus Gründen der leichten Lesbarkeit.

Die technischen Inhalte und Beschreibungen entsprechen dem Stand vom September 2009. Die Darstellung ist zeitabhängig und wird in folgenden Versionen neue Algorithmen, neue Speichermedien, mobile Platten mit anderer Technologie, etc. berücksichtigen.

INHALT:

1	EINLEITUNG	4
2	ABGRENZUNG VON MOBILEN DATENTRÄGERN	6
3	BESTEHENDE EMPFEHLUNGEN.....	8
4	USB-SPEICHERMEDIEN	8
4.1	Abgrenzung USB-Speichermedien	8
4.2	Umgang mit USB-Ports	9
4.3	Verschlüsselung von USB-Speichermedien	9
4.4	Maßnahmen bei Verlust.....	10
4.5	Fazit.....	11
5	OPTISCHE DATENTRÄGER	12
5.1	Abgrenzung optische Datenträger	12
5.2	Umgang mit optischen Lese-/Schreibgeräten	12
5.3	Verschlüsselung von Daten auf optischen Datenträgern	12
5.4	Maßnahmen bei Verlust.....	13
5.5	Fazit.....	13
6	NOTEBOOK, LAPTOP	14
7	BLACKBERRY, IPHONE, PDA.....	15
8	DATENTRÄGERAUSTAUSCH.....	15
9	ABKÜRZUNGSVERZEICHNIS.....	19
10	QUELLENVERZEICHNIS	19

1 EINLEITUNG

Neben der Abgrenzung und Nennung mobiler Datenträger werden im Dokument Hinweise gegeben, wie ein nach der Schutzbedürftigkeit der Daten erforderlicher und angemessener Schutz mobiler Datenträger vor unbefugtem Zugriff auf die dort gespeicherten Daten und möglichem Verlust der Datenträger hergestellt werden kann.

Das betrifft vor allem Daten mit personenbezogenen Inhalten als auch mit Inhalten zu Betriebs- und Geschäftsgeheimnissen. Im Dokument wird herausgestellt, dass eine Verschlüsselung der Daten auf mobilen Datenträgern im Allgemeinen erforderlich ist.

Weiter wird beschrieben, wie USB-Ports und USB-Speichermedien zu behandeln sind, um Daten sicher zu transportieren und vor unbefugter Einsichtnahme zu schützen. Das kann vom Verbot der USB-Schnittstellennutzung bis hin zur soft- oder hardwarekryptierten Lösung reichen. Verhaltensregeln beim Verlust eines USB-Speichermediums sind ebenfalls Bestandteil, wie auch Hinweise zur Nutzung an öffentlichen Rechnern (z. B. Internetcafé).

Diese Angaben werden im Weiteren außerdem für optische Datenträger gegeben.

Da auch Laptops, Notebooks und Netbooks zu den mobilen Datenträgern zählen, sind im Dokument Hinweise enthalten, wie mit USB-Schnittstellen, WLAN und Bluetooth-Komponenten zu verfahren ist. Möglichkeiten zur Festplattenverschlüsselung bzw. Partitionsverschlüsselung werden ebenfalls genannt. Diese mobilen Informationssysteme bergen eine Reihe weiterer Risiken in sich, auf die im vorliegenden Dokument aufgrund der breiten Gefährdungslage nicht eingegangen werden kann. Gleiches gilt für Geräte wie BlackBerry, PDA oder iPhone/Smartphone.

Die Empfehlungen, zum Teil den IT Grundschieckatalogen des BSI entnommen, sind nicht nur für das Behördenumfeld umsetzbar. Sie sind allgemeingültig und somit auch im Unternehmens- bzw. betrieblichen Umfeld anwendbar. Auch Privatpersonen können die im Weiteren aufgeführten Sicherheitshinweise, entsprechend angepasst, für ihre Informationstechnik übernehmen.

Die nachstehenden Maßnahmen gelten nicht nur für mobile Datenträger, die persönlich transportiert und genutzt werden. Für mobile Datenträger, die über DHL, Kuriere und sonstige

Versandwege das Behörden- bzw. Unternehmensumfeld¹ verlassen, werden im Dokument weitergehende Empfehlungen gegeben.

Alle im Dokument aufgeführten Maßnahmen können es ermöglichen, dass ein Verlust oder eine Manipulation von Daten auf mobilen Datenträgern erschwert oder sogar ganz verhindert wird.

¹ *Behörde zu Behörde, Behörde an Externe bzw. Externe an Behörde / Unternehmen an Unternehmen bzw. an Behörden weitere Externe, wie auch Privatpersonen*

2 ABGRENZUNG VON MOBILEN DATENTRÄGERN

Neben den Möglichkeiten Daten als Dokumente in Papierform bzw. Aktenlage für den Transport zu halten, hat sich die Speicherung auf magnetischen, elektronischen und optischen Datenträgern zunehmend etabliert.

Im Zuge der Entwicklung so genannter Flashspeicher sind die optischen und im Besonderen die magnetischen Medien - zumindest für Zwecke der Kurzzeitspeicherung und des Datentransportes - in den Hintergrund getreten.

Die USB-Speichermedien (USB-Sticks/ -Festplatten) gewinnen im Bereich der mobilen Datenträger immer mehr an Bedeutung. Gerade in Bezug auf Speicherkapazität und Komfort beim Transport besitzen sie einen hohen Stellenwert, da die Maße der USB-Speichermedien abnehmen und platzsparend befördert werden können. Dazu zählen ebenfalls die noch kleineren Flash-Karten, die nicht nur mit den entsprechenden Steckplätzen eines Systems verbunden werden können, sondern auch über USB-Adapter.

Aber auch Laptops, Notebooks bzw. Netbooks zählen zu den mobilen Datenträgern, da Daten ohne Zwischenspeicherung unterwegs komfortabel zur Verfügung stehen.

Aufgrund der Eigenschaft Daten zu speichern, gehören digitale Fotoapparate, MP3-Speichergeräte ebenso wie PDA's, iPhones, Mobiltelefone und BlackBerry zu mobilen Datenträgern.

Damit ergibt sich in der Zusammenfassung folgende Gruppe an mobilen Datenträgern:

- Laptops,
- Notebooks,
- Netbooks,
- Mobiltelefone,
- PDA,
- BlackBerry,
- iPhone, Smartphone,
- CD's / DVD's,

- Disketten/ Magnetbänder,
- USB-Sticks/ -Festplatten
- Flash-Karten,
- MP3-Speichergeräte,
- digitale Fotoapparate und Kameras.

Für die Gruppe der Notebooks, Laptops und Netbooks sowie für Mobiltelefone, BlackBerry, PDA, iPhone, SmartPhone als auch letztendlich für die MP3-Speichergeräte/ digitalen Bildgeräte beziehen sich die nachfolgenden Empfehlungen nur auf die Verwendung der USB-Schnittstellen und die darüber erfolgende Speicherung von Daten. Die restlichen Gruppen unterliegen zusätzlichen Gefährdungen, die hier nicht umfassend erläutert werden können.

Grundsätzlich gilt, dass gespeicherte, personenbezogene Daten auf mobilen Datenträgern, zu verschlüsseln sind, wenn sie außerhalb der Behörde oder des Unternehmens verarbeitet bzw. transportiert werden sollen (§ 22 Abs. 3 i. V. m. § 21 Abs. 2 Nr. 1 DSGVO).

Auf weitere Empfehlungen zu magnetischen Datenträgern nimmt dieses Dokument keinen Bezug. Für den Versand magnetischer Speichermedien gelten die Empfehlungen des Kapitels 8 (Datenträgeraustausch). Werden derartige Speichermedien nach Abschluss des Transports für andere Zwecke verwendet, sind die darauf gespeicherten Daten zu löschen. Dazu wird auf die Orientierungshilfe des LfDI M-V „Sicheres Löschen magnetischer Datenträger“ (<http://www.lfd.m-v.de>) verwiesen.

3 BESTEHENDE EMPFEHLUNGEN

Im letzten Absatz wurde bereits auf das Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V) eingegangen.

Nachfolgend wird auf die bundeseinheitlichen Empfehlungen des Arbeitskreises „Technische und organisatorische Datenschutzfragen“ verwiesen, die auf den Internetseiten des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern² als Orientierungshilfen³ zu finden sind (<http://www.lfd.m-v.de/download.html>).

Bei diesen Empfehlungen handelt es sich um folgende Orientierungshilfen:

- „Datensicherheit bei USB-Geräten“ mit Stand vom 16. November 2004;
http://www.lfd.m-v.de/dschutz/informat/usb/oh_dsusb.pdf,
- „Einsatz kryptografischer Verfahren“ in der Version 1.0 mit Stand vom September 2003; http://www.lfd.m-v.de/dschutz/informat/krypto/oh_krypt.pdf;
- „Datenschutzrechtliche Aspekte beim Einsatz optischer Datenspeicherung“ mit Stand aus dem Jahr 1995; http://www.lfd.m-v.de/dschutz/informat/optosp/oh_opto.html,
- „Sicheres Löschen magnetischer Datenträger“ mit Stand vom 07.10.2004;
<http://www.lfd.m-v.de/dschutz/informat/magloe/magloe.pdf>.

4 USB-SPEICHERMEDIEN

4.1 Abgrenzung USB-Speichermedien

Zu den USB-Speichermedien zählen:

- USB-Sticks/-Festplatten,
- Flash-Karten (SD/MMC, u.w. Karten) über USB-Port,
- digitale Fotoapparate und Kameras, MP3-Speichergeräte

² Im Weiteren *LfDI*

³ Im Weiteren *OH*

- PDA,
- BlackBerry und
- iPhone/Smartphone.

4.2 Umgang mit USB-Ports

Neben der Sperrung der USB-Ports über die BIOS-Einstellungen an stationärer und mobiler PC-Technik besteht die Möglichkeit, über Softwarelösungen restriktive Freigaben für USB-Speichermedien zu schalten. Eine Sperrung der USB-Ports über die BIOS-Einstellungen bzw. das Hardwareprofil sichert die Einhaltung des Verbotes der unbefugten Nutzung von USB-Speichermedien. Sie muss aber an jedem stationären bzw. mobilen Informationssystem vorgenommen werden. Dazu ist sicherstellen, dass das BIOS-Passwort nur den Administratoren bekannt ist. Eine später notwendige Freigabe an einem oder mehreren PC's erfordert ebenfalls die Kenntnis über das BIOS-Passwort und Eingreifen eines Administrators mit entsprechenden Rechten.

4.3 Verschlüsselung von USB-Speichermedien

Grundsätzlich gilt, dass gespeicherte, personenbezogene Daten auf mobilen Datenträgern, zu verschlüsseln sind, wenn sie außerhalb der Behörde oder des Unternehmens verarbeitet bzw. transportiert werden sollen (§ 22 Abs. 3 i. V. m. § 21 Abs. 2 Nr. 1 DSGVO).

Es wird jedoch nachdrücklich empfohlen, auch nicht personenbezogene Daten grundsätzlich auf USB-Speichermedien zu verschlüsseln. Die Verschlüsselung sollte unabhängig vom festgestellten Schutzbedarf und vom Kriterium der personenbezogenen Daten erfolgen.

Über die einzusetzende Softwarelösung muss gewährleistet sein, dass nur berechtigte und vom Unternehmen bzw. der Behörde zugelassene USB-Speichermedien vom System erkannt und aktiviert werden. „Fremde“, nicht verifizierte USB-Speichermedien, dürfen vom System nicht angenommen werden und sind mit einer entsprechenden Hinweismeldung zu sperren. Ein unberechtigtes Kopieren, Einlesen bzw. Schreiben von Daten darf nicht möglich sein.

Unabhängig vom Schutzbedarf bzw. der Art der Daten (z. B. personenbezogene Daten), sollten Daten beim Kopieren vom Informationssystem auf das zugelassene USB-Speichermedium,

mittels des Verschlüsselungsalgorithmus AES 256 kryptiert und somit gegen unbefugtes Auslesen geschützt werden. Eine mögliche Option, Daten ungesichert auf einem USB-Speichermedium zu transportieren, sollte nicht freigegeben werden.

Eine weitere Möglichkeit des verschlüsselten Speicherns von Daten auf USB-Speichermedien ist die Hardwarekryptierung. Hier ist von Vorteil, dass ein Lesen und Schreiben auf allen mobilen und stationären Informationssystemen möglich ist, also auch auf Informationssystemen außerhalb des Umfeldes der Behörde bzw. Unternehmens (Fremdsysteme).

4.4 Maßnahmen bei Verlust

Die vorgenannten Sicherheitsmaßnahmen können dem Verlust oder Diebstahl eines USB-Speichermediums nicht vorbeugen. Es kann durch die Verschlüsselungsmaßnahmen nur sichergestellt werden, dass ein unberechtigtes Auslesen der gespeicherten Daten verhindert bzw. erschwert wird. Bei Verlust bzw. Diebstahl eines USB-Speichermediums sind schnellstens Maßnahmen, im Rahmen eines Sicherheitsvorfallplanes (Incident Handling) der Behörde, dem Unternehmen, einzuleiten, um den potentiellen Missbrauch der betroffenen Informationen zu verhindern bzw. zu minimieren.

Dieser Plan muss enthalten:

- Meldewege: Wer hat an wen den Verlust zu melden.
- Wer ruft das Sicherheitsvorfallteam in welchem Umfang zusammen.
- Welche Schritte hat das Sicherheitsvorfallteam entsprechend der verlorengegangenen Daten zu unternehmen.
- Nachbereitung: Welche Sicherheitsmaßnahmen müssen zusätzlich für die Zukunft eingebunden werden.

Wird ein „verloren geglaubter“ mobiler Datenträger wieder „aufgefunden“, so ist er auf Manipulation bzw. Veränderungen zu prüfen, bevor er der weiteren Verwendung zugeführt wird. Hier ist es sinnvoll einen Integritätscheck (z. B. Prüfsummenverfahren) sowie einen Virencheck durchzuführen.

Je länger ein USB-Speichermedium „verschwunden“ ist, um so mehr besteht die Gefahr, dass mit genügend hoher krimineller Energie und Rechenleistung auch die dort enthaltenen Daten möglicherweise entschlüsselt und evtl. manipuliert wurden.

Derzeitig sind keine erfolgreichen Angriffe auf eine Verschlüsselung mit AES 256 Bit bekannt und weitgehend auszuschließen.

Die vorstehenden Maßnahmen gelten nicht nur für personalisierte USB-Speichermedien. Für USB-Speichermedien, die über DHL, Kuriere und weitere Versandwege das Behörden-Unternehmensumfeld⁴ verlassen, werden im Kapitel 8 (Datenträgeraustausch) weitergehende Empfehlungen gegeben.

4.5 Fazit

Soweit eine Sperrung von USB-Ports an stationärer bzw. mobiler PC-Technik nicht vorgesehen ist, sollte eine Kryptierung der Daten auf mobilen USB-Speichermedien mit mindestens 256 Bit AES-Verschlüsselung stattfinden. Die Verschlüsselung kann softwareseitig oder durch den Einsatz von hardwarekryptierten USB-Speichermedien erfolgen. Werden die USB-Ports der stationären bzw. mobilen PC-Technik nicht über das BIOS des entsprechenden Arbeitsplatz-PC gesperrt, muss eine Lösung zur restriktiven Rechtevergabe bzw. Steuerung der zuzulassenden USB-Speichermedien vorgenommen werden.

Verloren gegangene bzw. gestohlene und wieder aufgefundene USB-Speichermedien sind einer eingehenden Prüfung auf Manipulation zu unterziehen.

Die Nutzung von dienstlich eingesetzten USB-Speichermedien an öffentlicher Informationstechnik, z. B. Internetcafé, ist zu untersagen. Gleiches gilt für die private Nutzung.

⁴ *Behörde zu Behörde, Behörde an Externe bzw. Externe an Behörde / Unternehmen an Unternehmen bzw. an Behörden weitere Externe, wie auch Privatpersonen*

5 OPTISCHE DATENTRÄGER

5.1 Abgrenzung optische Datenträger

Die im Weiteren betrachteten optischen Datenträger beschränken sich auf den Bereich der:

- einmal beschreibbaren CD,
- wieder beschreibbaren CD,
- einmal beschreibbaren DVD,
- wieder beschreibbaren DVD.

5.2 Umgang mit optischen Lese-/Schreibgeräten

Soweit es für das betreffende System für die Erfüllung der Fachaufgabe nicht notwendig ist, sollten die Schreibzugriffe auf so genannte CD-/DVD-Brenner unterbunden werden. Auch wenn auf dem Informationssystem kein Brennprogramm installiert wurde, ist es unter einigen Windows-Betriebssystemen dennoch möglich Daten auf CD's bzw. DVD's über den Windows-Explorer und dessen integrierte Brenn-Engine zu schreiben.

Weiter empfiehlt sich, CD oder DVD-Laufwerke über die BIOS-Einstellungen bzw. im Hardwareprofil des stationären bzw. mobilen Systems zu deaktivieren, sobald sie für den Einsatz des Informationssystems im Bezug auf die Aufgabenerfüllung nicht benötigt werden. Bei stationären Systemen kann das entsprechende Laufwerk aus dem Informationssystem entfernt werden.

Externe optische Lese-/Schreibgeräte, die mittels USB-Anschluss an ein Informationssystem angeschlossen werden, sind zusätzlich zu den nachfolgenden Empfehlungen wie ein USB-Speichermedium (siehe Punkt 4) zu behandeln.

5.3 Verschlüsselung von Daten auf optischen Datenträgern

Da auf optischen Datenträgern eine Hardwareverschlüsselung wie unter Punkt 4.3 nicht möglich ist, wird eine softwarebasierende Verschlüsselungslösung auf der Basis AES 256, (Punkt 4.3) empfohlen.

Auch bei einer 256 Bit AES-Verschlüsselung der Daten auf optischen Datenträgern sind folgende Punkte zu beachten.

Werden einmal beschreibbare CD's oder DVD's nicht mehr benötigt, muss eine sichere Art der Datenträgervernichtung gewählt werden (u. a. Shredder).

Wieder beschreibbare CD's bzw. DVD's sind vor der weiteren Benutzung zu löschen (Formatierung). Dennoch kann nicht sichergestellt werden ob und vor allem welche Restinformationen auf dem optischen Speichermedium verbleiben.

5.4 Maßnahmen bei Verlust

Im Weiteren ist hier den Empfehlungen des Punktes 4.4 zu folgen.

Die vorstehenden Maßnahmen gelten nicht nur für optische Datenträger, die persönlich transportiert und genutzt werden. Für optische Datenträger, die über DHL, Kuriere und weitere Versandwege das Behörden- Unternehmensumfeld⁵ verlassen, werden im Kapitel 8 weitergehende Empfehlungen gegeben.

5.5 Fazit

Die Möglichkeit optische Datenträger zu lesen bzw. zu erstellen, ist von der Notwendigkeit der Erfüllung der Fachaufgabe abhängig zu machen. Ist ein CD bzw. DVD-Laufwerk nicht notwendig, so ist es aus dem Informationssystem auszubauen bzw. über das BIOS oder Hardwareprofil zu deaktivieren.

Sind Lese-/Schreibeinrichtungen für optische Datenträger zur Erfüllung der Fachaufgabe notwendig, so sind diese über restriktive Rechte im System bzw. über den Einsatz entsprechender Software zu steuern.

Soweit keine Sperrung von CD bzw. DVD-Laufwerken an stationärer bzw. mobiler PC-Technik vorgesehen ist, sollte eine Kryptierung der Daten auf optischen Datenträgern mit mindestens 256 Bit AES-Verschlüsselung erfolgen.

⁵ Behörde zu Behörde, Behörde an Externe bzw. Externe an Behörde / Unternehmen an Unternehmen bzw. an Behörden weitere Externe, wie auch Privatpersonen

6 NOTEBOOK, LAPTOP

Im Kapitel 2 wurde durch die Abgrenzung Mobiler Datenträger deutlich, dass auf Notebooks, Laptops und Netbooks näher eingegangen werden muss. Aufgrund der Breite der Gefährdungslagen kann sich eine Betrachtung in diesem Rahmen nur auf die USB-Schnittstellen, Schnittstellen zu optischen Lese-/Schreibgeräten und die Festplattenverschlüsselung erstrecken.

Für diese Informationssysteme ist im BIOS ein HDD-Passwort (Festplattenpasswort) zu vergeben. Dieses darf nur dem/den Nutzer/n und dem entsprechenden Administrator bekannt sein. Das BIOS ist ebenfalls durch ein entsprechendes Passwort zu schützen, dass nur dem Administrator bekannt sein darf. Für den Vertretungsfall und zur Notfall-Regelung sind die Passwörter sicher und unter Einhaltung restriktiver Rechte verschlossen zu lagern.

Notebooks/ Laptops neuerer Bauart verfügen zum Teil hardwareseitig über eine Festplattenverschlüsselung. Soweit die Geräte es vorsehen, sollte diese Verschlüsselung genutzt werden. Das Passwort darf nur dem/den Nutzer/n und dem entsprechenden Administrator bekannt sein. Für den Vertretungsfall und zur Notfall-Regelung ist das Passwort sicher und unter Einhaltung der Zugriffsrechte zu lagern, da sonst ein Zugriff auf die Daten nicht mehr gegeben ist (Datenverlust). Die Zugangsrechte beinhalten dabei Fragen, wie „Wer darf für welches Gerät die Zugangsdaten/ das Passwort erhalten?“ (Organisationsstruktur)

Zur Unterstreichung der Notwendigkeit einer Verschlüsselung wird hier noch einmal auf den auf den Absatz 3⁶ des § 22 DSGVO M-V verwiesen.

USB-Schnittstellen und Laufwerke für optische Datenträger sind entsprechend den Empfehlungen der Kapitel 4 und 5 zu behandeln.

Die WLAN-Möglichkeiten mobiler Informationssysteme sind auf den fachbezogenen Einsatz zu prüfen. Besteht keine zwingende Notwendigkeit für den WLAN-Einsatz, so ist diese Funktionalität zu sperren. Gleiches gilt für die Bluetooth-Schnittstelle.

Der Einsatz von Laptops, Notebooks und Netbooks an öffentlichen Orten ist in Abhängigkeit der fachbezogenen Aufgabe zu prüfen und ggf. zu untersagen. Aufgrund der Bauweisen von

⁶ Werden personenbezogene Daten mit Hilfe informationstechnischer Geräte von der verarbeitenden Stelle außerhalb ihrer Räumlichkeiten verarbeitet, sind die Datenbestände zu verschlüsseln.

modernen Mobiltelefonen, digitalen Fotoapparaten etc. ist ein unbemerktes Abfilmen des Bildschirminhaltes möglich.

7 BLACKBERRY, IPHONE, PDA

Ausgehend vom Kapitel 2 wurde durch die Abgrenzung mobiler Datenträger deutlich, dass auch BlackBerry, iPhone/Smartphone und PDA hier in den Fokus rücken müssen. Aufgrund der Breite der weiteren Gefährdungslagen kann sich eine Betrachtung in diesem Rahmen nur auf die USB-Schnittstellen der Geräte beschränken.

Für diese Geräte ist ein Passwortschutz einzurichten. Neben der notwendigen PIN-Eingabe bei BlackBerry und Mobiltelefonen bietet ein zusätzliches Passwort einen gewissen Schutz während des Betriebes. Geht ein eingeschaltetes Gerät verloren, kann ohne Passwort nicht auf die gespeicherten Daten zugegriffen werden. Ein unberechtigtes Telefonieren ist ebenfalls nicht möglich.

Eine Speicherkartenerweiterung (Flashkarten: siehe Kapitel 3) sollte untersagt bzw. technisch verhindert werden.

8 DATENTRÄGERAUSTAUSCH

Bereits im Vorfeld ist für den Datenträgeraustausch mit mobilen Datenträgern verbindlich festzulegen, mit welchem Kommunikationspartner und mit welcher Art von Daten und Datenträgern der Informationsaustausch innerhalb und außerhalb des Behörden-Unternehmensumfeldes erfolgen soll.

Für die verschiedenen Datenträger ist konzeptionell festzuhalten, welche Risiken diese in sich bergen und welche Sicherheitsmaßnahmen zu ergreifen sind.

In einer Datenträgerverwaltung ist u. a. zu klären:

- welche mobilen Datenträger für die Kommunikation genutzt werden können,
- welche Daten auf mobilen Datenträgern gespeichert werden dürfen bzw. welche nicht,

- wie die auf mobilen Datenträgern gespeicherten Daten vor unbefugtem Zugriff, Manipulation und Verlust geschützt werden sollten,
- mit welchen externen Kommunikationspartnern Datenträger ausgetauscht werden dürfen und welche Sicherheitsregelungen dabei zu beachten sind,
- wie verhindert wird, dass die mobilen Datenträger für die unbefugte Weitergabe von Informationen benutzt werden,
- wie gegen die Verbreitung von Schadsoftware über die mobilen Datenträger vorgebeugt wird.

Neben den Anforderungen der Datenträgerverwaltung muss sich auch die Versandart der Datenträger am vereinbarten Schutzbedarf und Gefährdungspotential orientieren. Je mehr Personen mit der Beförderung befasst, und je länger die Zeiten sind, in denen der Datenträger unbeaufsichtigt bleibt (z. B. Postweg), desto weniger kann im Allgemeinen für die Vertraulichkeit und Integrität garantiert werden. Dementsprechend sind angemessene Versandarten auszuwählen.

Dabei kann z. B. zwischen folgenden Versandarten gewählt werden:

- Post (mit verschiedenen Versandangeboten, die unterschiedliche Garantien für die Transportgeschwindigkeit und Absicherung umfassen),
- Kurierdienste,
- persönlicher Kurier und
- persönliche Übergabe.

In der Datenträgerverwaltung muss für die verschiedenen Datenträger, nach festgelegtem Schutzbedarf kategorisiert, eine angemessene Versandart vorgeschlagen werden. Die Liste der Versandarten in der Datenträgerverwaltung sollte mindestens folgende Aspekte berücksichtigen:

- durchschnittliche Transportzeit der Versandart bzw. des Kurier's
- Vertrauenswürdigkeit der Versandart bzw. des Kuriers,
- Kosten.

Weiterhin muss vereinbart werden, in welchen Behältern die Datenträger zu versenden sind.. Elektromagnetische Datenträger (Bänder, evtl. Disketten) müssen vor elektromagnetischen Einflüssen, optische Datenträger (CD/DVD) vor übermäßiger Erwärmung geschützt transportiert werden. Ein unberechtigtes Öffnen des Transportbehälters muss für die Kommunikationspartner sofort zu erkennen sein (z. B. Brechen eines Siegels).

Die Auswahl geeigneter Datenträger ist mit den Kommunikationspartnern abzustimmen. Dabei ist verbindlich festzulegen:

- Um welche Daten handelt es sich?
- Welches Datenvolumen soll gespeichert werden?
- Welche Aufbewahrungsfristen sollen durch den mobilen Datenträger abgedeckt werden?
- Sollen Daten „revisionssicher“ gespeichert werden?
- Welcher Schutzbedarf besteht (Kategorisierung nach BSI ...)?

Beim Datenträgeraustausch sind mehrere Schutzmaßnahmen zu beachten, um mögliche Schäden zu vermeiden bzw. die Schadensauswirkungen zu minimieren.

Dazu gehören die sichere Aufbewahrung und Verpackung der Datenträger sowie eine eindeutige Kennzeichnung, um eine mögliche Verwechslungsgefahr zu verringern.

Eine Überprüfung auf Computer-Viren vor dem Versenden oder der Übergabe und ebenfalls nach dem Empfang sollte zu den notwendigen Prozeduren beim Sender bzw. Empfänger der mobilen Datenträger gehören.

Personen-/ -unternehmensbezogene oder Wirtschaftsdaten sind grundsätzlich vor dem Transport bzw. der Übermittlung mit einem kryptographischen Verfahren zu verschlüsseln. Werden weitere Informationen übertragen, deren Integrität und/oder Vertraulichkeit über den normalen Schutzbedarf hinausgehen bzw. besteht eine gewisse Möglichkeit, dass die Informationen Unbefugten zur Kenntnis gelangen, manipuliert oder durch technische Fehler verändert werden können, ist ein kryptographisches Verfahren zum Schutz der Daten für den Transport oder die Übermittlung zu nutzen (, siehe Punkt 4.3 und Punkt 5.3). Der Einsatz einer digitalen Signatur ist im Einzelfall zu überdenken bzw. bei über dem normalen Schutzbedarf hinausgehender Schutzbedürftigkeit zu nutzen.

Wenn USB-Speichersticks mit unterschiedlichen Kommunikationspartnern ausgetauscht werden, sind diese vor ihrer erneuten Verwendung physikalisch zu löschen, um die Übermittlung von Informationsresten an den falschen Empfänger zu vermeiden.

Eine für den normalen Schutzbedarf ausreichende physikalische Löschung kann erreicht werden, indem der komplette Datenträger mit einem bestimmten Muster überschrieben wird. Möglich ist auch eine Formatierung des Datenträgers, wenn sie nicht wieder rückgängig gemacht werden kann.

Das Löschen von einzelnen Daten ist zu vermeiden. Hierbei bleiben in der Regel Restinformationen erhalten, die eine Rekonstruktion der gelöschten Dateien ermöglichen.

Wieder beschreibbare CD's oder DVD's können grundsätzlich durch vollständiges Überschreiben gelöscht werden. Laut Recherchen ist aber nicht bekannt, ob trotzdem Spuren der alten Informationen verbleiben und rekonstruiert werden können. Bei erhöhtem Schutzbedarf sollten deshalb auch wieder beschreibbare Datenträger mit geeigneten Geräten vernichtet werden, um die darauf gespeicherten Informationen sicher zu löschen.

Es kann nie ausgeschlossen werden, dass Datenträger beim Transport verloren gehen.

Die übermittelten Daten sollten so lange in Kopie vorgehalten werden, bis der korrekte Empfang des Datenträgers bestätigt wurde. Je nach Zweck des Datenträgeraustausches kann auch eine längere Speicherung der Kopie als Beweismittel für spätere Konflikte erforderlich sein.

Bei Ausfall, Defekt, Zerstörung oder Diebstahl eines mobilen Datenträgers muss der Vorfall umgehend - entsprechend den Regelungen des Sicherheitsvorfallmanagements (Behandlung von Sicherheitsvorfällen) - gemeldet werden. Die Verfahrens- und Meldewege müssen den Kommunikationspartnern bekanntgegeben werden. Bei einem Diebstahl ist entsprechend schnell zu handeln, um den potentiellen Missbrauch der betroffenen Informationen zu verhindern. Wird ein „verloren geglaubter“ mobiler Datenträger wieder „aufgefunden“, so ist er auf Manipulation bzw. Veränderungen zu prüfen, bevor er der weiteren Verwendung wieder zugeführt wird.

Für personenbezogene Daten, vor allem im Bereich des hohen und sehr hohen Schutzbedarfes, ist unter Berücksichtigung der infrastrukturellen Gegebenheiten die Übertragung über das CN LAVINE vorzuziehen. Eine 256 Bit AES-Verschlüsselung sollte dort ebenfalls genutzt werden. Der Einsatz einer digitalen Signatur ist im Einzelfall schutzbedarfsabhängig zu überdenken.

9 ABKÜRZUNGSVERZEICHNIS

AES	Advanced Encryption Standard, ein symmetrisches Kryptosystem
CD	Compact Disc
DVD	Digital Versatile Disc
LfdI	Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern
OH	Orientierungshilfe
PC	Personalcomputer
PDA	Personal Digital Assistant
USB	Universal Serial Bus

10 QUELLENVERZEICHNIS

<http://www.bsi.de>

<http://www.lfd.m-v.de>

IT-Grundschutzkataloge BSI, 10. Ergänzungslieferung

BSI-Standard 100-1 – Managementsysteme für Informationssicherheit (ISMS), Version 1.5

BSI-Standard 100-2 – IT-Grundschutz-Vorgehensweise, Version 2.0

BSI-Standard 100-4 – Notfallmanagement, Version 1.0