Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

46.629.2

Handreichung zum einfachen und sicheren Datentransport mit Wechseldatenträgern

Stand: November 2018

Friedrichstr. 219
10969 Berlin
Besuchereingang:
Puttkamer Str. 16-18

Telefon: (030) 13889-0
Telefax: (030) 215 50 50
mailbox@datenschutz-berlin.de

Sprechzeiten

tgl. 10-15 Uhr, Do. 10-18 Uhr
(oder nach Vereinbarung)

Erreichbarkeit

U6: Kochstr.
Bus: M29, 248

Internet

https://datenschutz-berlin.de

Einleitung

Wechseldatenträger wie USB-Sticks und tragbare, externe Festplatten sind eine einfache und bequeme Möglichkeit um Daten von einem Computer zu einem anderen zu transportieren. Wenn hierbei personenbezogene Daten transportiert werden, sollten diese jedoch verschlüsselt werden. So sind die Daten geschützt, auch wenn der Datenträger verloren geht oder gestohlen wird.

Alle Vereine, Unternehmen, öffentliche Einrichtungen und anderen Organisationen innerhalb der europäischen Union sind verpflichtet, angemessene technische Maßnahmen zum Schutz von personenbezogenen Daten zu ergreifen. Diese Handreichung soll die Organisationen bei der Erfüllung ihrer Pflichten unterstützen. Sie richtet sich primär an kleine Organisationen mit einem geringen Grad an Professionalisierung. Insbesondere bei großen Organisationen oder besonders sensitiven Daten sollten zusätzliche Maßnahmen ergriffen werden.

Verschlüsselung von Datenträgern mit Windows BitLocker

In verschiedenen Versionen von Windows ist die Software „BitLocker“ enthalten. Diese kann unter Anderem eingesetzt werden, um USB-Sticks oder tragbare Festplatten zu verschlüsseln. BitLocker bietet eine aus technischer Sicht ausreichende Sicherheit.

Eine Anleitung zur Nutzung findet sich (im September 2018 noch nicht auf Deutsch übersetzt) unter *https://docs.microsoft.com/de-de/windows/security/information-protection/bitlocker/bitlocker-basic-deployment*. Weitere (auch deutschsprachige) Anleitungen finden sich in online verfügbaren Artikeln handelsüblicher Computer-Zeitschriften. BitLocker ist verhältnismäßig anwenderfreundlich und leicht zu bedienen.

BitLocker-Verschlüsselung kann jedoch nur auf Computern mit dem Windows-Betriebssystem verwendet werden. Beim Datentransport zu Computern mit einem anderen Betriebssystem (etwa Linux oder Mac OS) kann BitLocker nicht eingesetzt werden. Mit Windows 10 wurde darüber hinaus ein neuer Verschlüsselungsmodus eingeführt, der von älteren Windows-Versionen nicht unterstützt wird. Wenn absehbar ist, dass Datenträger nur an Computern mit Windows 10 verwendet wird, sollte der neuere Verschlüsselungsmodus gewählt werden.

Verschlüsselung mit VeraCrypt

VeraCrypt ist eine kostenlos verfügbare Verschlüsselungssoftware, die unter *https://www.veracrypt.fr/en/Downloads.html* heruntergeladen werden kann. VeraCrypt wird sowohl für Windows-Systeme als auch für Linux- und Mac-OS-Systeme angeboten und eignet sich daher gut zum verschlüsselten Datentransport zwischen Computern mit verschiedenen Betriebssystemen. VeraCrypt bietet die Möglichkeit, Daten entsprechend dem Stand der Technik zu verschlüsseln. Verglichen mit BitLocker ist VeraCrypt in der Bedienung jedoch etwas komplexer.

Mit VeraCrypt können wahlweise ganze Laufwerke verschlüsselt werden oder verschlüsselte „Container“ angelegt werden. Dies sind verschlüsselte Dateien, innerhalb derer andere Dateien und Ordner abgelegt werden können. Solche Container können über die Funktion „Create Volume“ angelegt werden. Bestehende Container können über die Funktion „Mount“ geöffnet werden und stehen anschließend als eigenes Laufwerk zur Verfügung. Kopiert oder verschiebt man Dateien auf dieses Laufwerk, so werden die Dateien von VeraCrypt automatisch verschlüsselt in der Container-Datei abgelegt. Über die Funktion „Dismount“ wird ein Container wieder geschlossen.

Genauere Anleitungen zur Benutzung von VeraCrypt finden sich z.B. unter *https://www.veracrypt.fr/en/Beginner's Tutorial.html* (auf Englisch) und in diversen Artikeln handelsüblicher Computer-Zeitschriften.

Verschlüsselung durch Selbstverschlüsselnde Laufwerke

Manche Hersteller von USB-Sticks oder tragbaren Festplatten bieten Datenträger an, die speziell für den verschlüsselten Datentransport entworfen wurden und daher über besondere Sicherheitsfunktionen verfügen. Die tatsächlich gebotene Sicherheit ist von Produkt zu Produkt unterschiedlich und für Laien nur schwer zu bewerten. Einen wertvolle Bewertungsgrundlage können Zertifikate des Bundesamts für Sicherheit in der Informationstechnik bieten. Beispielsweise kann bei Produkten, die den Schutzprofilen „BSI-CC-PP-0081-2012 - Portable Storage Media Protection Profile“ (*https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0081.html*) oder „BSI-PP-0025-2006 - Schutzprofil für USB-Datenträger“ (*https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0025.html*) entsprechen, von einer ausreichenden Sicherheit ausgegangen werden. Aussagekräftig sind auch Zertifizierungen anderer unabhängiger Zertifizierungsstellen nach FIPS 140-2 Level 3. Schließlich können auch ausführliche Produkttests von angesehenen Computer-Fachzeitschriften Anhaltspunkte geben.

Wahl eines starken Passworts

Die Sicherheit der verschlüsselten Dateien hängt direkt von der „Stärke“ des verwendeten Passworts ab. Je schwieriger ein Passwort zu erraten ist, desto „stärker“ ist das Passwort und desto sicherer sind die verschlüsselten Daten. Einfache Wörter („Schiff“), Namen von Familienmitgliedern („Paul“), Arbeitskollegen („Alina“) oder Haustieren („James“), Geburtsdaten, regelmäßig Buchstabenfolgen („abcdef“) oder Tastenfolgen („qwertz“) sind keine ausreichend sicheren Passwörter. Daran ändern auch einfache Verfremdungen wie z.B. das Anfügen von Zahlenkombinationen („James83“, „5Paul67“) oder das Ersetzen von Buchstaben durch Ziffern oder Sonderzeichen („@l1na“) nicht viel. Angreifer können mit spezieller Software und entsprechender Hardware ohne Weiteres Millionen bis Milliarden möglicher Passwörter binnen Minuten ausprobieren. Wörterbücher und Listen gebräuchlicher Namen sind frei verfügbar, einfache Verfremdungen wie oben beschrieben können von den Softwares automatisch durchgeführt werden und die verfremdeten Wörter in die Suche einbezogen werden.

Ein starkes Passwort sollte vor allem zwei Eigenschaften erfüllen: Es sollte möglichst lang sein und möglichst zufällig sein. Dies bedeutet insbesondere, dass es nicht mit der Person, die es verwendet, zusammenhängen sollte – auch nicht indirekt. Eine einfache Methode um starke Passwörter zu wählen ist z.B. das zufällige Auswählen von mehreren Wörtern aus einem Wörterbuch (z.B. „Haus jenseits Pflanze sammeln Zoo Geschichte warm Solarplexus“). Ein solches Passwort ist leichter zu merken als kryptische Kombinationen aus Buchstaben, Zahlen und Sonderzeichen („t7Xj+%e//2-P)b“) und trotzdem relativ sicher. Die Berliner Beauftragte für den Datenschutz und Informationsfreiheit empfiehlt die Verwendung von mindestens 8 zufällig gewählten Wörtern. Wer lieber mit zufälligen Zeichenkombinationen arbeitet, dem wird eine Mindestlänge von 14 Zeichen empfohlen.

Passwort-Manager

Da viele Menschen Schwierigkeiten haben, sich eine Vielzahl von verschiedenen Passwörter zu merken, ist grundsätzlich der Einsatz eines Passwort-Managers zu empfehlen. Ein Passwort-Manager ist ein Programm, mit dem sich die eigenen Passwörter verschlüsselt abspeichern lassen. Meist wird zur Speicherung eine Datei verwendet, die auch als „Passwort-Datenbank“ bezeichnet wird. (Passwort-Manager, die die verschlüsselten Passwörter zu einem Internet-Dienst hochladen oder automatisch zwischen verschiedenen Rechnern synchronisieren können, sollten sicherheitshalber vermieden werden.) Zur Entschlüsselung der Passwörter wird ein separates Passwort, das „Master-Passwort“ verwendet. Da über dieses Master-Passwort der Zugang zu allen anderen Passwörtern möglich ist, sollte unbedingt ein sehr starkes Master-Passwort gewählt werden.
Es gibt verschiedene kommerziell verfügbare sowie kostenlose Passwort-Manager. Vergleiche und Bewertungen finden sich in handelsüblichen Computer-Fachzeitschriften.
In einem Passwort-Manager können neben Passwörtern zur Entschlüsselung von Datenträgern auch Passwörter für den Zugang zu Online-Diensten und Ähnlichem abgelegt werden.

Nutzung dedizierter Laufwerke

Nach Möglichkeit sollten nur von der IT-Stelle vorbereitete und freigegebene USB-Sticks oder Laufwerke zum Transport personenbezogener Daten verwendet werden. Die Verwendung anderer USB-Datenträger sollte nach Möglichkeit technisch unterbunden werden. Dies dient auch der Vermeidung der Beeinträchtigung von Computern durch manipulierte Datenträger. Insbesondere sollten private USB-Sticks nicht für den Transport personenbezogener Daten verwendet werden.

Wenn besonders sensitive personenbezogener Daten transportiert werden sollen, sollten nur vom Bundesamt für Sicherheit in der Informationstechnik zertifizierte USB-Laufwerke verwendet werden. Alternativ sollte man zu Gunsten von wiederbeschreibbaren CDs und DVDs vollständig auf den Einsatz von USB-Laufwerken verzichten. Auch beim Datentransport mit CDs und DVDs ist eine sichere Verschlüsselung jedoch in der Regel unerlässlich.