Technisches und rechtliches Rezertifizierungs-Gutachten - Kurzgutachten -

Einhaltung datenschutzrechtlicher Anforderungen durch das Produkt "TeamDrive 2.4"

für:

TeamDrive Systems GmbH
Hamburg

erstellt von:

Andreas Bethke
Dipl. Inf. (FH)
Beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannter Sachverständiger für IT-Produkte (technisch)

Papenbergallee 34
25548 Kellinghusen
tel 04822 – 37 89 05
fax 04822 – 37 89 04
mob 0179 – 321 97 88
email bethke@datenschutz-guetesiegel.sh

Stephan Hansen-Oest
Rechtsanwalt
Beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannter Sachverständiger für IT-Produkte (rechtlich)

Neustadt 56
24939 Flensburg
tel 0461 – 90 91 356
fax 0461 – 90 91 357
mob 0171 – 20 44 98 1
email sh@hansen-oest.com

Stand:
August 2011

A. Einleitung

Die TeamDrive Systems GmbH (nachfolgend: TDS) strebt die Rezertifizierung ihres Produktes „TeamDrive“ für das Gütesiegel für IT-Produkte des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) an.

Die Vorlage eines rechtlichen und technischen Gutachtens ist Voraussetzung für die Rezertifizierung des Produktes. Dieses Dokument dient als Gutachten zur Vorlage beim ULD im Zusammenhang mit der Rezertifizierung des Produktes.

Dem Gutachten wird der Anforderungskatalog in der Version 1.2 zugrunde gelegt.

Das Gutachten stellt die Zusammenfassung der von den Sachverständigen vorgenommenen Prüfungen dar und berücksichtigt insbesondere die Neuerungen/Änderungen des Produktes sowie eine etwaige geänderte Rechtslage. Auf die Unterlagen, die im Zusammenhang mit der Erstzertifizierung vom 14.03.2005 sowie den Rezertifizierungen vom 14.03.2007 und 06.03.2009 zugrunde gelegt wurden, wird Bezug genommen.

B. Zeitpunkt der Prüfung

Die Prüfung des Produktes fand vom 17.02.2011 bis zum 04.08.2011 statt.

C. Detaillierte Bezeichnung des IT-Produktes

Das Produkt „TeamDrive“ wurde vom Hersteller entwickelt, um den einfachen, sicheren und schnellen Austausch von Daten (Dateien aller Art) zwischen zwei oder beliebig vielen Computern über das Internet oder über interne Netzwerke zu ermöglichen. Dabei agieren die Anwender in Gruppen um auf einen gemeinsamen Datenbestand, den sog. „SharedSpace“ (im Folgenden kurz: „Space“) zuzugreifen. Das Produkt verfügt über ein Berechtigungskonzept, mit dem die differenzierte Vergabe von Lese- bzw. Lese- und Schreibrechten ermöglicht wird. Über eine Administratorfunktion werden der „Space“ sowie die Benutzer der jeweiligen Gruppe verwaltet.

Der Datenbestand stellt sich dem Benutzer, der eine Client-Software installiert hat, als neues virtuelles Laufwerk dar. Sobald eine Datei dort gespeichert ist, haben alle Mitglieder der Gruppe entsprechend ihrer Berechtigung (Lesen oder Ändern) Zugriff.

D. Änderungen und Neuerungen des Produktes

Eine Veränderung der Prozesse der Schlüsselgenerierung, des Schlüsseltausches und der Serverkommunikation ist auch bei der neuen Version 2.4 nicht vorgenommen worden.

Neu ist, dass es nun auch Client-Software für das Betriebssystem Mac OS X und Linux gibt. Eine Änderung des Produktes selbst geht damit jedoch nicht einher. Lediglich die Oberfläche sieht anders aus. Es werden auf allen Betriebssystem-Varianten die gleichen Komponenten verwendet. Die Portierung in das jeweilige Betriebssystem führt nach Auffassung der Gutachter zu keiner Änderungen der technischen oder rechtlichen Betrachtung.

In technischer Hinsicht ist lediglich unter Mac OS X ein zusätzlicher Daemon-Dienst erforderlich gewesen, der dafür sorgt, dass Benachrichtigungen („notifications“) auch ohne Root-Rechte von dem Client verarbeitet und dargestellt werden können. Der Daemon-Dienst selbst stellt aufgrund seiner Struktur und Funktionsweise keine Beeinträchtigung der Sicherheit und/oder Funktionalität des Produktes dar.

Neben der Windows, Mac OS und Linux-Version gehört auch die „TeamDrive Portable (Windows)“-Version zum Prüfgegenstand. Diese ist im Kern und der Funktion identisch mit der Windows-(nicht Portable)-Version. Der Hersteller empfiehlt für diese Version im Handbuch, dass Benutzer ihre Geräte entsprechend schützen. Dies kann z.B. durch Passwortschutz, Truecrypt oder einer andere geeignete Verschlüsselungstechnologie geschehen, da TeamDrive selbst - im Falle des Verlustes des USB-Sticks - nicht vor dem unberechtigten Zugriff auf die Daten schützt. Sollte der USB-Stick ungeschützt verloren gegangen sein empfiehlt der Hersteller, dass der für den Space zuständige Benutzer die Zugriffsmöglichkeiten des Benutzers, der seinen USB-Stick verloren hat, zu entfernen.

Weitere Neuerungen:

I. Cloud Hosting

Seit der Version 2.3 gibt es die Möglichkeit, einen Shared-Space auf eigenen Servern (siehe II.) oder aber in der sog. „Amazon-Cloud“ anzulegen.

Seit Anfang März 2011 wird die Cloud-Lösung auch in Deutschland angeboten.

Amazon betreibt seine Cloud-Services in verschiedenen Ländern. Es gibt neben der US-Cloud auch eine „europäische Cloud“, wobei TDS grundsätzlich die europäische Cloud nutzt, bei der Amazon die Verarbeitung der Daten auf Servern in einem EU-Mitgliedsstaat garantiert.

Standardmäßig nutzen alle Kunden die EU-Cloud. Kunden außerhalb von Europa haben die Möglichkeit eine entsprechende Vereinbarung mit TeamDrive über die Nutzung der Amazon US oder ASIA Cloud zu treffen.

Der Benutzer erhält dann einen "Space" auf einem europäischen Server. Der Benutzer wird hierüber im Handbuch des Herstellers in ausreichender Weise informiert.

TDS speichert die Inhalte von der TeamDrive-Spaces von Benutzern von TeamDrive auf Amazon-Systemen ausschließlich in verschlüsselter Form. Die Daten sind sowohl während des Transports als auch auf den Systemen selbst jederzeit verschlüsselt. Eine Entschlüsselung erfolgt nur in den Endgeräten der Benutzer selbst.

Für die Verschlüsselung werden in den EC2-Systemen von Amazon EBS-Volumes angelegt, die mittels virtueller, verschlüsselter Festplatten mit EncFS-Technologie vor dem unbefugten Zugriff geschützt werden. Es werden nicht nur Dateiinhalte, sondern auch Dateinamen verschlüsselt.

Die verwendeten technischen Maßnahmen sind nach Auffassung der Gutachter geeignet, eine dem Stand der Technik entsprechende Sicherheit der Daten vor unbefugten Zugriffen Dritter zu gewährleisten.

Die Zertifizierung durch das Datenschutz-Gütesiegel erstreckt sich nur auf die Nutzung von Servern, die sich in Europa befinden.

II. Speicherung auf eigenem Server

In der aktuellen Version können Daten auch auf einem eigenen Server gespeichert werden. Hierzu werden die beiden Varianten „TeamDrive Personal Server“ und „TeamDrive Enterprise Server“ angeboten. Diese Produkte sind unabhängig vom TeamDrive zu sehen und nicht Gegenstand der Zertifizierung.

III. LDAP-Anbindung

Auf der Webseite des Herstellers wird im "TeamDrive Professional" Paket eine LDAP-Anbindung als optionale Funktion angeboten. Diese ist nicht Bestandteil der Zertifizierung.

IV. Eigenes Passwort beim Erstellen von Spaces

Mit Nutzung der neuen Version ist es nun möglich, für einen selbstangelegten Space ein eigenes Passwort zu vergeben, das für die Einladung und einen ersten Zugang zum Space genutzt wird. Der Anbieter empfiehlt in seiner Produktdokumentation die zusätzliche Nutzung von Passwörtern für die Spaces, um einen unberechtigten Zugriff auf Daten zu verhindern. Diese neue Passwortfunktion steht für alle aktuellen Versionen („Free“, „Personal“ und „Professional“) zur Verfügung.

V. Versionsunterschiede zwischen den TeamDrive-Versionen

Mit der Rezertifizierung sollen nun alle Client-Versionen das Gütesiegel bekommen. Um der Daten verarbeitenden Stelle den Einsatz einer geeigneten Version von TeamDrive zu erleichtern, hat der Hersteller auf seiner Webseite eine entsprechende Gegenüberstellung der drei Versionen (TeamDrive Free, TeamDrive Personal und TeamDrive Professional) mit ihren jeweiligen Leistungsmerkmalen veröffentlicht. Darüber hinaus sollen hier die funktionellen Unterschiede dargestellt werden:

Unterschiede der TeamDrive Personal-Version im Vergleich zur TeamDrive Free-Version:

a) keine Bannerwerbung
b) keine Speicherplatzbegrenzung im Client

Unterschiede der TeamDrive Professional-Version im Vergleich zur TeamDrive Personal-Version:

a) Beim Anlegen eines Spaces kann der Nutzer selbst entscheiden, wie viele Versionen einer Datei auf dem Server gespeichert werden sollen ("unlimitiert", "limitiert auf 10 Versionen", "limitiert auf 5 Versionen", "limitiert auf 3 Versionen", "limitiert auf 1 Version")

b) Veröffentlichung von einzelnen Dateien über eine URL:
Hierbei wird die Datei erneut (allerdings in unverschlüsselter Form) auf einen TeamDrive Cloud oder Personal Server hochgeladen, und es wird eine URL erzeugt. Diese URL kann dann per Mail etc. weitergegeben werden. Der Benutzer kann die hochgeladene Datei jederzeit löschen. Die Datei wird anschließend nicht mehr verändert, auch wenn die (Ursprungs-)Datei im TeamDrive geändert wird. Es gibt keinen automatischen Austausch der veröffentlichten Datei.

c) Versenden von Kommentaren per E-Mail:
In der TeamDrive Professional Version kann der Benutzer einen Kommentar an die Teammitglieder per E-Mail versenden. Der Inhalt wird unverschlüsselt übertragen. Allerdings weist der Hersteller hierauf direkt im Client durch eine Meldung an den Benutzer hin.

d) Übertragung von Metadaten:
Beim Annehmen einer Einladung in einen Space kann der Benutzer entscheiden, ob von seinen Dateien nur die Metadaten übertragen werden. In diesem Fall bleiben Dateien mit einer Größe mit mehr als 100 Kilobyte auf dem Server.

Folgende Metadaten werden übertragen: Dateiname, Ordnername, Spacename, Username, Datum der Änderung, Version Nr, Vorgänger Version

e) Cache-Einstellungen :
TeamDrive hat einen lokalen Cache, in der die Versionen zu den Dateien lokal gespeichert werden (in früheren Versionen hieß dieser Cachespeicher „Archiv“). Mit der Einführung der Bezeichnung „Cache“ wurde eine Einstellbarkeit der Größe ermöglicht. In der Free- und der Personal-Version ist die Größe fest auf 500 MB eingestellt. Werden mehr Versionen erzeugt, sind diese dann nur auf dem Server gespeichert.

Alle Daten werden auf dem Weg ins Archiv/Cache verschlüsselt und komprimiert. Anschließend werden die Daten verschlüsselt zum Hosting-Server übertragen. Nach erfolgreicher Übertragung auf den Hosting-Server werden die Daten je nach eingestellter Cache-Größe lokal gelöscht. Wenn der Cache auf 0 eingestellt ist, befindet sich nur die aktuelle Version einer Datei im Dateisystem. Der Nutzer kann in den Einstellungen > erweiterten Einstellungen den Cache löschen (nur ab Professional-Version). Zu diesem Zweck kann die gewünschte Cachegröße von 0 bis x eingestellt werden. Anschließend muss der Nutzer noch den Menüpunkt "bereinigen“ auswählen, um die Aktion auszuführen. Wenn alte Versionen auf dem Server gelöscht werden, wird eine Information hierzu auch an den Client gesendet. Wenn die Version im TeamDrive Papierkorb endgültig gelöscht wird, wird diese auch aus dem Cache entfernt.
Nach dem Leeren des TeamDrive Papierkorb (endgültig löschen) werden die Dateien auf dem Server und im Cache gelöscht.

E. Datenschutzrechtliche Bewertung

Cloud Hosting

Sofern personenbezogene Daten im Auftrag eines deutschen Unternehmens in "Clouds" verarbeitet werden, stellt dies nach überwiegender Auffassung eine Verarbeitung von Daten im Auftrag dar, die nach Maßgabe des § 11 BDSG rechtlich zu bewerten ist.

Für die rechtliche Beurteilung der Nutzung von Cloud-Services durch TDS ist entscheidend, ob überhaupt personenbezogene Daten im Auftrag von TDS durch Amazon verarbeitet werden. Dies ist bei näherer Betrachtung jedoch grundsätzlich nicht der Fall. Alle in den sog. Spaces abgelegten Daten werden verschlüsselt an die Server in der "Cloud" übertragen und werden dort auch nur verschlüsselt verarbeitet. Amazon selbst hat keinerlei Möglichkeit, eine Entschlüsselung der Daten vorzunehmen. Aufgrund der fehlenden Möglichkeiten, einen Personenbezug aus den Daten herzuleiten, weisen die Daten, die Amazon für TDS speichert grundsätzlich keinen Personenbezug für Amazon auf. Allerdings wäre es denkbar, dass Amazon während der Laufzeit durch vertragswidrige Maßnahmen oder auf gerichtliche Anforderung oder Anforderung einer Sicherheitsbehörde Kenntnis von Daten erhalten kann, die einen Personenbezug aufweisen können. Dabei handelt es sich jedoch ausschließlich um Anmeldedaten wie den Nutzernamen und die E-Mail-Adresse.

Aufgrund der besonderen rechtlichen Situation bei Nutzung der Amazon-Cloud kann zurzeit nicht ausgeschlossen werden, dass US-Sicherheitsbehörden Zugriff auf personenbezogene Daten zur Laufzeit des Systems erhalten. Dies betrifft jedoch allenfalls – wie bereits aufgeführt - die Anmeldedaten. Auf die übertragenen Daten aus dem TeamDrive Client kann kein Zugriff erfolgen. Alle 256 Bit AES-Schlüssel, die erforderlich sind, um auf die Daten zuzugreifen, sind ausschließlich auf den Client-Computern gespeichert. Amazon und andere Dritte haben keine Möglichkeit die gespeicherten Daten zu entschlüsseln. Auch ist eine Entschlüsselung während der Laufzeit ausgeschlossen.

Die technische Bewertung des Verschlüsselungsvorgangs ist bereits mehrfach vom technischen Sachverständigen geprüft und auch beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein für zulässig erachtet worden.

Es bestehen weder in technischer noch in rechtlicher Hinsicht Bedenken gegen den Einsatz der Amazon-Cloud in der von TDS umgesetzten Form mit einer Vollverschlüsselung der Daten.

TDS hat zudem am 29.04.2011 vorsorglich eine vertragliche Vereinbarung über die Verarbeitung von Daten im Auftrag mit der Amazon Web Services LLC (AWS) geschlossen. Dabei handelt es sich um das „AWS Enterprise Customer Agreement“, in das ein „Exhibit 3.3.3 - AWS Data Processing Addendum (Germany)“ als Anlage wirksam vertraglich einbezogen wurde.

In diesem Zusammenhang wird von Bedeutung, dass TDS die EU-Cloud von Amazon benutzt. Denn dadurch, dass dann die Verarbeitung von Daten nicht in einem Drittstaat erfolgt, wird eine Auftragsdatenverarbeitung in zulässiger Form möglich (vgl. § 3 Abs. 8 BDSG). Sofern eine Verarbeitung personenbezogener Daten in einem Drittstaat stattfinden würde, wäre die verarbeitende Stelle "Dritter" im Sinne des Gesetzes; eine Auftragsdatenverarbeitung käme dann nicht mehr in Betracht.

Nach Ziff. 3.2 des Exhibits 3.3.3. („AWS Data Processing Addendum (Germany)“) kann TDS festlegen, dass die Verarbeitung von Daten in der EU (konkret: Irland) stattfindet. Dies hat TDS in seinem Verfahren entsprechend geregelt. Die Voraussetzungen für das Vorliegen einer Auftragsdatenverarbeitung liegen daher vor. Die Verarbeitung von etwaigen personenbezogenen Daten kann ausschließlich in der EU erfolgen.

Um eine zulässige Auftragsdatenverarbeitung annehmen zu können, müssten die weiteren Voraussetzungen des § 11 BDSG eingehalten werden. Die zwischen TDS und Amazon geschlossenen Verträge sind im Zuge der Rezertifizierung im Hinblick auf die Einhaltung der Vorgaben des § 11 BDSG und insbesondere des Kataloges aus § 11 Abs. 2 BDSG geprüft worden. Nach Auffassung der Gutachter werden die Voraussetzungen einer zulässigen Auftragsdatenverarbeitung im Falle von TDS und Amazon eingehalten.

Auftragsdatenverarbeitungsvertrag zwischen TDS und Kunden

Auch wenn im Einzelfall fraglich sein kann, ob bei der Nutzung von TDS durch Endkunden eine Verarbeitung von Daten im Auftrag vorliegt, hält TDS ein Vertragsmuster zur Auftragsdatenverarbeitung für Endkunden vor. Da TeamDrive in der Regel von nichtöffentlichen Stellen bzw. Privatnutzern genutzt wird, basiert der Vertrag auf den Anforde-

rungen des § 11 BDSG. Da die Anforderungen des § 17 LDSG-SH jedoch nicht über die des § 11 BDSG hinausgehen und es einer öffentlichen Stelle möglich ist, einen eigenen Auftragsdatenverarbeitungsvertrag mit eigenen Inhalten mit TeamDrive zu schließen, ist nachfolgend nur eine Prüfung nach Maßgabe des § 11 BDSG erfolgt.

Der den Kunden von TDS zur Verfügung gestellte Mustervertrag ist im Zuge der Rezertifizierung geprüft worden. Alle Voraussetzungen des § 11 BDSG und insbesondere des § 11 Abs. 2 BDSG werden eingehalten.

Versenden von E-Mail-Daten im Klartext

Für Zwecke der besseren Nutzbarkeit des Dienstes bietet TDS für sein Produkt jetzt an bestimmten Stellen die Möglichkeit, Kommentare zu Dokumenten per E-Mail zu versenden. Aufgrund der technischen Bedingungen der EC2-Infrastruktur von Amazon wird für das Versenden der E-Mail, die im Klartext übertragen werden, ein Dienstleister von TDS in Anspruch genommen. Dabei handelt es sich um die MCS Moorbek Computer Systeme GmbH („MCS“) aus Hamburg. Mit MCS besteht ein Auftragsdatenverarbeitungsvertrag, der nach der rechtlichen Prüfung, die im Zuge der Rezertifizierung durchgeführt worden ist, alle Voraussetzungen an ein rechtlich zulässiges Auftragsdatenverarbeitungsverhältnis i.S.d. § 11 BDSG erfüllt.

Sonstige Neuerungen

Die Einführung neuer Linux- und Mac OS X-Oberflächen führt zu keiner anderen rechtlichen und technischen Bewertung. Es kommen die gleichen Komponenten zum Einsatz, die lediglich betriebssystemspezifisch portiert wurden. Lediglich die Dateiüberwachung („Notifications“) ist betriebssystemspezifisch geregelt. Unter Linux kommt hierfür das ab Kernel 2.6x mitgelieferte „inotify“ zum Einsatz. Unter Mac OS X kommt ein eigens von TDS entwickelter Event-Deamon („TeamDriveFSEventDeamon“) zum Einsatz, der erforderlich war, da ansonsten ohne Root-Rechte die Dateibenachrichtigungsdienste unter Mac OS X nicht funktionsfähig wären.

Die Möglichkeit der Speicherung auf eigenen Servern ist nicht Gegenstand der Zertifizierung. Eine Bewertung entfällt daher.

Die neue Möglichkeit, ein eigenes Initialpasswort für einen selbst erzeugten Space zu generieren und separat an die Teilnehmer verschicken zu können, wird als positiv bewertet, da hierdurch noch mehr Sicherheit und Flexibilität für die individuellen Sicherheitsanforderungen der Nutzer erreicht werden kann. In der Professional-Version gibt es jetzt auch die Möglichkeit, Daten über einen URL Dritten verfügbar zu machen. Dabei sind diese Dateien dann unverschlüsselt. Hier ist der Nutzer aufgefordert, nur Daten zugänglich zu machen, die keine personenbezogenen Daten enthalten, bzw. entsprechende Pseudonymisierungen vorzunehmen.

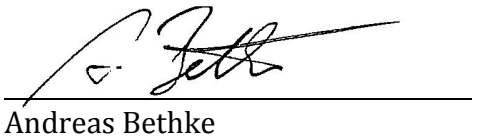
Auch beim Versenden von Kommentaren per E-Mail, die im Klartext erfolgt, sollte der Nutzer darauf achten, dass keine personenbezogenen Daten übermittelt werden. Auch wenn es nicht in der rechtlichen Verantwortung von TDS liegt: wenn dennoch personenbezogene Daten auf Veranlassung des Nutzers versendet werden, weist TDS die Nutzer auf diese Umstände in der Dokumentation und bei der Nutzung der Funktion im Programm selbst hin, was wiederum vorbildlich ist.

F. Zusammenfassung

Insgesamt kann festgestellt werden, dass auch mit dem neuen Produkt die Rechtsvorschriften zu Datenschutz und Datensicherheit eingehalten werden.

Hiermit bestätige ich, dass das oben genannte IT-Produkt den Rechtsvorschriften über den Datenschutz und die Datensicherheit entspricht.

Kellinghusen, den 04.08.2011



Andreas Bethke

Flensburg, den 04.08.2011

Stephan Hansen-Oest