Technisches und rechtliches Rezertifizierungs-Gutachten - Kurzgutachten -

Einhaltung datenschutzrechtlicher Anforderungen durch das Produkt "TeamDrive 3"

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:
13.10.2013

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, 06.03.2009 und 05.08.2011 zugrunde gelegt wurden, wird Bezug genommen.

B. Zeitpunkt der Prüfung

Die Prüfung des Produktes fand vom 23.05.2013 bis zum 27.09.2013 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.
Die Verschlüsselung der Daten erfolgt clientseitig. Es handelt sich somit um eine sogenannte „end-to-end"-Verschlüsselung.
TeamDrive setzt auf die folgenden Verschlüsselungsmechanismen:

- **Advanced Encryption Standard – AES 256**
  Zur Verschlüsselung der Daten setzt TeamDrive auf das Advanced Encryption Standard (AES) Kryptosystem mit einem 256 Bit Schlüssel und verwendet die C Code Implementation der OpenSSL library.
- **Diffie-Hellman und RSA 3072**
  Für den Schlüsselaustausch setzt TeamDrive bei seinen älteren Clients auf den Diffie-Hellman Algorithmus. Neue Clients hingegen verwenden RSA 3072 (s. unten). Die Diffie-Hellman Implementierung basiert dabei auf der C Code Implementation wie sie von der OpenSSL library zur Verfügung gestellt wird.
- **Message Digest 5/6 – MD5/MD6**
  Der TeamDrive Hash-Funktionalität liegt der MD5 bzw. MD6 Algorithmus zu Grunde, wobei der Hashwert mit einer zufällig gewählten Zeichenfolge (Salt) gespeichert wird.
- **PrimeBase Privacy Guard – PBPG**
  Der PrimeBase Privacy Guard (PBPG) ist ein proprietäres Public/Privat Schlüsselsystem, das auf dem Diffie-Hellman Schlüsselaustausch und der AES Verschlüsselung aufsetzt. Das Verhalten von PBPG für den Anwender gleicht dem bekannten Public/Privat Schlüsselsystemen von PGP oder GnuPG. Die PBPG-Verschlüsselung generiert zufällige Änderungen und verifiziert die Dateien während des Austauschs, damit PBPG erkennen kann, ob eine Nachricht oder ein Schlüssel manipuliert oder anderweitig verändert worden sind. Zwei Nachrichten sind dabei niemals gleich. Dabei wird nicht nur für jeden Benutzer ein Schlüsselpaar erzeugt, sondern ebenfalls für jede Installation. Die PBPG Implementierung ist offen und kann bei Bedarf von Partnern und anderen Interessierten überprüft werden.

Nicht Teil des Zertifizierungsgegenstandes sind die für iOS- und Android-Systeme verfügbaren Apps. Diese dort verwendeten Verschlüsselungsmechanismen sind zwar identisch mit denen der Desktop-Applikationen, so dass insoweit nach hiesiger Auffassung keine grundlegenden Bedenken gegen eine Nutzung dieser Smartphone-Apps bestehen. Die Begutachtung von Apps auf iOS- und Android-Systemen bedarf jedoch weiterer Prüfungen und soll ggf. im Zuge einer Rezertifizierung erfolgen.

D. Änderungen und Neuerungen des Produktes

Mit der Version 3 von TeamDrive wurde der Algorithmus für den Schlüsselaustausch angepasst. Das Diffie-Hellmann Verfahren wurde durch RSA 3072 ersetzt. Durch die höhere Verschlüsselung besteht nun keine Kompatibilität mehr mit älteren Clients und somit zu den Spaces, die mittels eines Clients der Version 2 erzeugt und verwaltet wurden. Beide Versionen können jedoch parallel betrieben werden. Eine Einladung kann aber nicht versionsübergreifend geschehen. Der Hersteller empfiehlt den Anwendern, die Spaces von Version 2 auf Version 3 zu migrieren. Dies ist derzeit nicht automatisch möglich. Die Anwender haben jedoch die Möglichkeit, die Dateien aus den alten Spaces (V2) in neu angelegte Spaces (V3) manuell zu kopieren und die bestehenden Nutzer aus den alten Spaces entsprechend wieder neu in die neuen Spaces (V3) einzuladen.

E. Datenschutzrechtliche Bewertung

Die Veränderung der Algorithmus für den Schlüsselaustausch ist positiv zu bewerten. Bereits 2003 veröffentlichte die RSA Laboratorien eine Prognose für die Lebensdauer von Schlüssellängen ihres eigenen RSA-Algorithmus[1]. Demnach gilt die Schlüssellänge von 3072 bit auch nach dem Jahr 2030 als „sicher“. Bezüglich der Sicherheit wäre der bislang verwendete Diffie-Hellmann mit einem 3072-bit Schlüssel genau so sicher, jedoch dauert die Generierung einer sicheren Primzahl (die für den Algorithmus nötig ist) ca. 18 Minuten auf einem – immer noch weit verbreiteten – Intel Core2Duo Prozessor.[2]

Im Hinblick auf die Einhaltung der Anforderungen aus § 6 LDSG zu Protokolldaten kann festgestellt werden, dass die Anforderung in organisatorischer Weise adäquat umgesetzt werden kann. Wenn ein Space gelöscht wird, werden automatisch alle Daten und auch die dazugehörigen Protokolldaten gelöscht. Verlässt ein Benutzer einen Space, so bleiben die Daten natürlich erhalten. Gleiches gilt für die Sekundärdaten („Logs“ im Space). Sollen diese Daten gelöscht werden, so müssen die Primärdaten in einen anderen Space übertragen werden. Mit dem Löschen des alten Spaces werden dann die Protokolldaten gelöscht.

[1] http://www.rsa.com/rsalabs/node.asp?id=2004
[2] Vgl. http://www.cryptopp.com/wiki/Diffie-Hellman

In rechtlicher Hinsicht hat es keine Änderungen der einschlägigen rechtlichen Vorschriften gegeben. Insoweit war eine Neubewertung nicht erforderlich.

Eine Neuerung hat es noch in den Datenschutzhinweisen im TeamDrive Handbuch gegeben. Um auch Berufsgeheimnisträgern i.S.d. § 203 StGB erweiterte Hinweise zu einer rechtskonformen Nutzung von TeamDrive zu geben, wurde das Handbuch um folgenden Passus erweitert:

> ***7.1 Hinweis für Daten von Berufsgeheimnisträgern i.S.d. § 203 StGB***
> *TeamDrive ist generell zur Speicherung und zum Teilen von Daten und Informationen, die einem Berufsgeheimnis i.S.d. § 203 StGB unterliegen, geeignet. Die verwendeten Verschlüsselungsverfahren und -technologien schützen vor einem unbefugten Zugriff durch Dritte.*
> *Ein unbefugter Zugriff i.S.d. § 203 StGB kann in der Regel nur dann erfolgen, wenn ein menschliches Fehlerverhalten vorgekommen ist und z.B. falsche Berechtigungen und Freigaben auf einen Space vergeben wurden.*
> *Wir raten Ihnen in Verbindung mit dem Einsatz von TeamDrive als Berufsgeheimnisträger dazu, unseren zusätzlichen Passwortschutz zu verwenden. Durch den zusätzlichen Passwortschutz muss vor dem Versenden einer Einladung ein Passwort eingegeben werden. Dieses Passwort muss dem Empfänger auf einem unabhängigen, separaten Weg mitgeteilt werden. Der Empfänger muss dann beim Annehmen der Einladung das Passwort eingeben. Sie sollten dabei ein hinreichend langes und komplexes Passwort verwenden, um den höchstmöglichen Schutz für Ihre Daten zu gewährleisten.*

Wie schon im Erstgutachten ausgeführt[3], ist das Produkt auch für die Verarbeitung von Daten, die einem Berufsgeheimnis i.S.d. § 203 StGB unterliegen, geeignet. Dies soll auf

[3] Vgl. Rdnr. 73 im Erstgutachten: *„Die Verarbeitung der sog. **Inhaltsdaten** mit dem Produkt erfolgt in zulässiger Weise. Aufgrund der verwendeten Verschlüsselungsmechanismen können sowohl Daten mit „normalem" Schutzniveau als auch Daten mit sensitiven Informationen verarbeitet werden. Daten, die besonderen Berufsgeheimnissen i.S.d. § 203 StGB unterliegen, können ebenfalls mit dem Produkt in zulässiger Weise verarbeitet werden. Zwar ist ein unbefugte Offenbarung an nicht berechtigte Dritte nicht gänzlich ausgeschlossen; eine Offenbarung kann aber nur bei menschlicher Fehlbedienung erfolgen. So ist es zwar theoretisch denkbar, dass eine unbefugte Person durch eine Fehlbedienung bei der „Einladung" in einen SharedSpace Kenntnis von „Geheimnissen" i.S.d. § 203 StGB erlangt. Diese Fehlbedienung ist jedoch nicht unmittelbar auf das Produkt zurück zu führen.*

Wunsch des Produktherstellers konkret auch noch einmal in diesem Kurzgutachten erwähnt werden. In dem Zusammenhang wurde das Handbuch noch weiter verbessert. Gegen den Einsatz des Produktes durch Berufsgeheimnisträger bestehen in datenschutzrechtlicher Hinsicht keine Bedenken.

F. Zusammenfassung

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

Das Produkt selbst bietet auf Basis der verwendeten Verschlüsselungsverfahren hinreichenden Schutz vor der unbefugten Kenntnisnahme Dritter und ist damit sowohl für die Verarbeitung von Daten mit „normalem" Schutzniveau wie auch für sensitive Daten mit hohem Schutzniveau (z.B. bei Berufsgeheimnissen) geeignet."

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

Kellinghusen, den 23.10.2013

Andreas Bethke

Flensburg, den 23.10.2013

Stephan Hansen-Oest