Technisches und rechtliches Rezertifizierungs-Gutachten - Kurzgutachten -

Einhaltung datenschutzrechtlicher Anforderungen durch das Produkt "TeamDrive 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 – 36 63 000
fax 04822 – 36 63 333
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:
20.05.2016

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 2.0 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, 05.08.2011 und 22.10.2013 zugrunde gelegt wurden, wird Bezug genommen.

B. Zeitpunkt der Prüfung

Die Prüfung des Produktes fand vom 01.09.2015 bis zum 20.05.2016 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 mit CBC und PKCS7 padding und verwendet die C Code Implementation der OpenSSL library.
- **RSA 2048/3072**
  Für den Schlüsselaustausch verwendet TeamDrive beim aktuellen Client auf der Clientseite 2048-bit-Schlüssel und auf der Serverseite 3072-bit-Schlüssel für den RSA Algorithmus. Auch hier wird die C Code Implementation der OpenSSL library verwendet.
- **bcrypt**
  Der TeamDrive Hash-Funktionalität liegt der bcrypt Algorithmus zu Grunde, wobei der Hashwert mit einer zufällig gewählten Zeichenfolge (Salt) gespeichert wird. Zudem wird die „overtime-Funktion" benutzt, die das „Knacken" mittels Rainbow-tables erschwert und verlangsamt.
- **Message Digest 5 – MD5**
  An einer Stelle wird zur Generierung eines Hashwertes der MD5-Algorithmus verwendet. Dabei geht es um die Verifikation eines Clients für einen bestimmten Space.
- **PrimeBase Privacy Guard – PBPG**
  Der PrimeBase Privacy Guard (PBPG) ist ein proprietäres Public/Privat Schlüsselsystem, das auf dem bcrypt 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 späteren Rezertifizierung erfolgen.

D. Änderungen und Neuerungen des Produktes

Mit der Version 4 von TeamDrive wurden keinerlei Veränderungen an den grundlegenden Funktionen oder den Verschlüsselungsalgorithmen vorgenommen. Lediglich die Oberfläche wurde auf ein neues Design angepasst.
Geändert wurde die Auswahl für den Server. Neben der bestehenden Auswahl die verschlüsselten Daten auf einem eigenen Server, oder in der Amazon-Cloud in Irland zu speichern, gibt es nun die Möglichkeit ein Rechenzentrum in Deutschland zu wählen. Dabei handelt es sich um das „NBG6" der noris network AG aus Nürnberg. Nähere Informationen können unter
http://www.datacenter.de/de/rechenzentren/standorte/nbg-6/index.html abgerufen werden.
Aufgrund der Entscheidung des EuGH wird eine abschließende Beurteilung der Nutzung der Amazon Cloud erst bis zum 30.06.2016 erfolgen können und insoweit wird zunächst auf die Zertifizierung vom 22.10.2013 verwiesen. Sollte aufgrund der Rechtssituation nach dem 30.06.2016 trotz Verschlüsselung und bestehender Verträge mit Amazon für europäische Kunden kein ausreichender Datenschutz vorhanden sein, wird TeamDrive alle Daten der bestehenden Kunden aus den europäischen Datenzentren von Amazon in ein nach deutschem Recht betriebenes und BSI zertifiziertes Datacenter, das die Einhaltung aller deutschen und europäischen Datenschutz-, Datensicherheit und Compliance-Bestimmungen einhält, durchführen. Hierzu hat das Unternehmen einen „Replicator" entwickelt mit dem der Umzug aller Daten automatisiert an einen anderen Speicherort erfolgen kann.

E. Datenschutzrechtliche Bewertung

Die eingesetzten Verschlüsselungsmechanismen entsprechen aus Sicht der Gutachter immer noch dem Stand der Technik und sind auch vor dem Hintergrund der „Snowden-Enthüllungen" (NSA hat Zugriff auf SSL-Verschlüsselung) durch die doppelte Verschlüsselung mittels RSA 3072 immer noch als sicher einzustufen.

Die Erweiterung des Ortes der Speicherung ist positiv zu bewerten, da es sich um einen Anbieter aus Deutschland handelt, der entsprechenden deutschen Gesetzen unterliegt. Zudem kann das Rechenzentrum NBG6 der noris network entsprechende Zertifikate im

Bezug auf die Sicherheit vorweisen. Allen voran das ISO 27001 Zertifikat auf Basis von IT-Grundschutz des BSI (Bundesamt für Sicherheit in der Informationstechnik) mit der Nummer „BSI-IGZ-0177-2014“, das bis 26.05.2017 ausgestellt ist. Darüber hinaus wurde das Informationssicherheits Managementsystem nach ISO/IEC 27001:2005 für die Geltungsberiche „Lösungen, Produkte und Services in den Bereichen IT-Outsourcing, Cloud-Services, Managed Services, Network & Security sowie Rechenzentrumsinfrastrukturen und –betrieb“ bis 03.06.2016 von der DQS GmbH zertifiziert. Der Vertrag für eine Auftragsdatenverarbeitung wurde geprüft und nicht beanstandet.

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

Seit der letzten Rezertifizierung wurde der Anforderungskatalog des ULD Gütesiegels angepasst. Darum soll an dieser Stelle die neue tabellarische Darstellung erfolgen.

Anforderung nach Katalog oder sonstigen Rechtsnormen	**Bewertung**	**Kommentare**
Komplex 1:		
1.1 IT-Sicherheits-Schutzziele: Verfügbarkeit, Integrität, Vertraulichkeit	vorbildlich	
1.2 Datenschutz-Schutzziel: Nicht-Verkettbarkeit (inkl. Datensparsamkeit, Zweckbindung und Zwecktrennung)	vorbildlich	
1.3 Datenschutz-Schutzziel: Transparenz (inkl. Produktbeschreibung)	vorbildlich	
1.4 Datenschutz-Schutzziel: Intervenierbarkeit	vorbildlich	
1.5 Anpassung des IT-Produkts	adäquat	
1.6 Privacy by Default	adäquat	
1.7 Sonstige Anforderungen	entfällt	
Komplex 2:		
2.1.1 Gesetzliche Ermächtigung zur Verarbeitung der Daten	adäquat	
2.1.2 Einwilligung des Betroffenen	adäquat	
2.1.3.1 Vorschriften über die Datenerhebung	adäquat	
2.1.3.2 Vorschriften über die Übermittlung	adäquat	
2.1.3.3 Löschung nach Wegfall des Erfordernisses	adäquat	
2.2.1 Zweckbindung und Zweckänderung	adäquat	
2.2.2 Erleichterung der Umsetzung des Trennungsgebotes	adäquat	
2.2.3 Gewährleistung der Datensicherheit (§§ 5, 6 LDSG, Anlage zu § 9 BDSG)	vorbildlich	-
2.3 Datenverarbeitung im Auftrag	adäquat	-
2.4.1 gemeinsame Verfahren/Abrufverfahren	adäquat	-
2.4.2 Trennung der Verantwortlichkeiten	adäquat	-
2.4.3 Veröffentlichungen im Internet	adäquat	
2.4.4 Weitere besondere technische Verfahren	adäquat	

Anforderung nach Katalog oder sonstigen Rechtsnormen	Bewertung	Kommentare
2.5.1 Erleichterung bzw. Unterstützung von Pseudonymität und des Pseudonymisierens	adäquat	
Komplex 3:		
3.1.1. Physikalische Sicherung	Entfällt bzw. adäquat	obliegt dem Nutzer bzw. dem RZ-Betreiber
3.1.2 Authentisierung	adäquat	
3.1.3 Autorisierung	adäquat	
3.1.4 Protokollierung	vorbildlich	
3.1.5 Verschlüsselung und Signatur	vorbildlich	Alle personenbezogenen Daten werden verschlüsselt
3.1.6 Pseudonymisieren	entfällt	
3.1.7 Anonymisieren	entfällt	
3.2.1.1 Verfügbarkeit	vorbildlich	
3.2.1.2 Integrität	vorbildlich	
3.2.1.3 Vertraulichkeit	vorbildlich	
3.2.1.4 Nicht-Verkettbarkeit	entfällt	
3.2.1.5 Transparenz	vorbildlich	
3.2.1.6 Intervenierbarkeit	adäquat	
3.2.1.7 Protokollierung von Datenverarbeitungsvorgängen	vorbildlich	
3.2.1.8 Test und Freigabe	adäquat	
3.2.2 Erleichterung der Vorabkontrolle	adäquat	
3.2.3 Erleichterung bei der Erstellung des Verfahrensverzeichnisses	adäquat	
3.2.4 Benachrichtigungspflicht bei unrechtmäßiger Kenntniserlangung von Daten	entfällt	
3.2.5 Unterstützung der Tätigkeit des behördlichen Datenschutzbeauftragten		
3.3.1 Verschlüsselung	vorbildlich	
3.3.2 Anonymisierung oder Pseudonymisierung	entfällt	
3.3.3.1 Mobile Datenverarbeitungssysteme	entfällt	
3.3.3.1 Video-Überwachung und –Aufzeichnung	entfällt	
3.3.3.1 Automatisierte Einzelentscheidungen	entfällt	
3.3.3.1 Veröffentlichungen im Internet	entfällt	
3.4 Pflichten nach Datenschutzverordnung (DSVO), insbesondere für Verfahren	adäquat	
3.5 Anforderungen an den Betrieb bei Auftragsdatenverarbeitung	adäquat	
3.6 Sonstige Anforderungen	entfällt	
Komplex 4:		
4.1 Aufklärung und Benachrichtigung	adäquat	
4.2 Benachrichtigung des Betroffenen bei unrechtmäßiger Kenntniserlangung von Daten	adäquat	
4.3 Auskunft	adäquat	
4.4.1 Berichtigung	adäquat	
4.4.2 Vollständige Löschung	adäquat	
4.4.3 Sperrung	adäquat	
4.4.4 Einwand bzw. Widerspruch gegen die Verarbeitung	adäquat	
4.3.5 Gegendarstellung	adäquat	
4.5 Sonstige Anforderungen	entfällt	

Wie schon im Erstgutachten ausgeführt[1], ist das Produkt auch für die Verarbeitung von Daten, die einem Berufsgeheimnis i.S.d. § 203 StGB unterliegen, geeignet. Dies soll auf 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.

[1] 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. 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 20.05.2016

Andreas Bethke

Flensburg, den 20.05.2016

Stephan Hansen-Oest