Sichere Cloud-Collaboration für Unternehmen nach EU-DSGVO

TeamDrive Systems GmbH
Max-Brauer-Allee 50
D-22765 Hamburg
Phone +49 389 044 33
E-Mail: info@teamdrive.com
Web: www.teamdrive.com

Inhaltsverzeichnis

1 Executive Summary

Für viele Unternehmen und Anwender stellt die Cloud etwas Abstraktes dar. Viele Unternehmen speichern ihre Daten nicht mehr ausschließlich auf firmeninternen Server, sondern speichern ihre Daten und Dokumente in der Cloud. Aber Cloud ist nicht gleich Cloud: Es gibt mehrere Cloud-Optionen, Daten und Dokumente in der Cloud zu speichern. Ebenso ist ein Provider nicht gleich ein Provider: Wenn Daten nicht mehr auf eigenen Servern sondern in der Cloud gespeichert werden, ergeben sich viele Fragen:

- Wo werden meine Daten gespeichert?
- Wer kann auf meine Daten zu greifen?
- Wie sicher sind meine Daten?
- Was muss hinsichtlich des Datenschutzes beachten werden?
- Wo werden meine Daten gespeichert?

Und Anwendersoftware ist nicht gleich Anwendersoftware: Software für die Datensynchronisation und das Teilen von Daten und Dokumenten unterscheidet sich in ihrem „Look-and-feel“, in ihren Funktionen, ihrer Benutzerfreundlichkeit und vor allem in ihren Sicherheitsaspekten.
IT-Sicherheit und Datenschutz sind für Unternehmen, die Daten, Dokumente und Kundendaten in der Cloud speichern und verarbeiten, zu Recht von zentraler Bedeutung. Ziel der IT-Sicherheit ist es, Daten und Dokumente auf dem lokalen Rechner, dem Transportweg und in den Rechenzentren vor dem unbefugten Zugriff Dritter, z. B. durch Cyber-Attacken sowie vor Viren, Ransomware oder Trojanern zuverlässig zu schützen. Hierfür müssen bestimmte Vorgaben und Gesetze eingehalten werden, wie z. B. die Persönlichkeitsrechte nach dem Bundesdatenschutzgesetz, europäischen Richtlinien oder unternehmenseigene Datenschutzregeln. Für deutsche Cloud-Provider wie die TeamDrive Systems GmbH mit Rechenzentren am Standort Deutschland gelten sehr hohe Datenschutz-Anforderungen.

Neben der Sicherheit in der Cloud erfordert auch die Sicherheit der Datenübermittlung und der Datenintegrität hohe Aufmerksamkeit. In der Sync&Share-Software TeamDrive findet die Datenkommunikation zwischen lokalen Rechnern, mobilen Endgeräten und den Servern im Rechenzentrum des Providers stets Ende-zu-Ende-verschlüsselt statt. Alle Schlüssel verbleiben ausschließlich unter der Kontrolle des Benutzers. Dank der neuen Sicherheitslösung Point in Time Recovery (PiTR) erstellt TeamDrive in regelmäßigen Zeitabständen Datenwiederherstellungspunkte, sogenannte Snapshots. Auf Ihre Snapshots können Sie zu jedem Zeitpunkt im Schadensfall, wie z. B. bei einer defekten Festplatte oder bei einem Virenbefall, zurückgreifen und eine aus einem Snapshot erstellte Version Ihrer Daten mit wenig technischem und zeitlichem Aufwand wiederverwenden. Zusätzlich zu den Snapshots werden von TeamDrive vollständige, redundante Datensicherungen in der Cloud erstellt.

Nach fast vierjähriger Debatte haben der Europäischer Rat, das Europäisches Parlament und die Europäische Kommission über den endgültigen Inhalt der neuen EU-Datenschutz-Grundverordnung (DSGVO) geeinigt. Die neue Verordnung ist am 25. Mai 2016 in Kraft getreten und ersetzt die bereits seit 1995 geltende EU-Datenschutzrichtlinie (Richtlinie 95/46/EG). Die Verordnung sah eine Übergangszeit von zwei Jahren vor und gilt damit ab dem 25. Mai 2018 verbindlich in der gesamten Europäischen Union.
Das Inkrafttreten der EU-DSGVO am 28. Mai 2018 beinhaltet zahlreiche Neuerungen für die Verwendung und Speicherung personenbezogener Daten. Ab diesem Zeitpunkt sind Unternehmen verpflichtet, ein Datenschutzmanagement einzuführen, um personenbezogene Daten zu sichern. Wer gegen die Vorgaben des DSGVO verstößt, muss mit drakonischen Strafen rechnen, die neben finanziellen Einbußen auch einen Image-Schaden für Unternehmen nach sich ziehen. Jeder, der geschäftsmäßig mit personenbezogenen Daten Dritter umgeht, tun gut daran, sich mit den neuen Vorschriften auseinanderzusetzen und sich darauf einzustellen, was in Zukunft gelten wird, um einen kräftigen Bußgeldbescheid zu vermeiden. Die in TeamDrive verwendete Ende-zu-Ende-Verschlüsselung reduziert Bußgeldrisiken und Meldepflichten im Schadensfall und schützt damit nicht nur Ihre Daten, sondern auch die Verantwortlichen und die Geschäftsführer.

2 Cloud Computing – Zukunft der Datenhaltung

2.1 Unbegründete Angst vor der Cloud

Cyberangriffe sind heute keine Ausnahme mehr, aber sie sind nicht in erster Linie Cloud-spezifisch. Am 25. September 2017 wurde bekannt, dass sich Hacker über einen offenbar nicht ausreichend geschützten Administrator-Account Zugang zu den Datenbanken der Deloitte Limited verschafft haben. Der gehackte Administrator-Account war offenbar nur mit einem einzigen Passwort und nicht mit einer zweistufigen Autorisierung, wie bei solchen sicherheitsrelevanten Zugängen normalerweise üblich, geschützt gewesen. Danach konnten die Hacker auf Passwörter, Benutzernamen, Gesundheitsdaten oder andere sensible Daten von Top-Kunden der Unternehmensberatung zugreifen, berichtet der "Guardian"[1]. Die Täter sollen monatelange in großem Stil Datensätze entwendet haben.

Anfang September 2017 wurde bekannt, dass in den Vereinigten Staaten das größte der drei bedeutenden Wirtschaftsauskunfteien Equifax Corporation Opfer eines Datendiebstahls wurde. Unbefugte hatten sich im Zeitraum von Mai 2017 bis zum Zeitpunkt der Entdeckung des Datendiebstahls am 29. Juli 2017 unrechtmäßigen Zugriff auf sensible Daten von 143 Millionen US-Amerikanern – 44 % der amerikanischen Bevölkerung – verschafft. Dazu kommen weitere Opfer in Kanada, Großbritannien und Nordirland. Hierbei erlangten die Hacker Zugriff auf personenbezogene Daten wie Sozialversicherungsnummern, Geburtsdaten, Adressen sowie Kreditkarten- und Führerscheinnummern.[2]

Der Angriff auf Equifax Corporation gilt als der bis dato größte Diebstahl von Sozialversicherungsnummern. Der Angriff wurde durch eine Sicherheitslücke in einer Webanwendung des Unternehmens ermöglicht, die in den Internetauftritt des Konzerns eingebunden war. Wie hoch der Gesamtschaden neben dem Imageschaden für Equifax Corporation ausfällt, ist zum jetzigen Zeitpunkt noch nicht absehbar.

Dieses ist nicht der erste Fall von Datendiebstahl im großen Umfang. Bereits 2013 wurde die Handelskette Target Corporation gehackt; es wurden 40 Millionen Kreditkartennummern entwendet. Der Gesamtschaden wurde auf etwa 300 Millionen US Dollar beziffert. Die kanadische Target-Tochter konnte sich von dem Image-Schaden nicht mehr erholen und musste Insolvenz anmelden.

Und doch setzen noch viele Unternehmen auf On-Premise-Lösungen – also auf die Datenhaltung in den eigenen Räumlichkeiten. Besonders Sicherheitsbedenken und Datenschutzgründe verunsichern Verantwortliche und halten Unternehmen von der hybriden Datenspeicherung ab. Dabei können mit den richtigen Sicherheitslösungen sensible Daten in der Cloud Dank standardisierter Datensicherungsverfahren und definierter Service Level Agreements sicher geschützt werden.

Neben Sicherheitsfragen zählt zu den Gründen auch die Angst vor Abhängigkeit von einem Anbieter. Doch diese Angst ist völlig unbegründet, denn inzwischen haben sich Cloud Anbieter etabliert, es gibt zahlreiche Vorteile für Cloud-Computing und Datenmigrationen zwischen Cloud-Anbietern sind erprobt und fast ohne Downtime möglich. In Deutschland nutzen immer mehr kleine und mittelständige Unternehmen die Vorteile des Cloud-Computing; in 2016 waren es bereits knapp zwei Drittel der deutschen klein und mittleren Unternehmen (KMU)[3] wie aktuelle Zahlen belegen.

2.2 Sicherheit - Pro und Contra des Cloud-Computing

Fragt man die Verantwortlichen, werden häufig Sicherheitsargumente gegen eine Cloud-Lösung angeführt: Zu unsicher sei der Datenverkehr über das Internet zu den Rechenzentren. Doch genau das Gegenteil ist der Fall: Welches kleine oder mittlere Unternehmen betreibt einen vergleichbaren Sicherheitsaufwand, den

---

[1] https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails?CMP=twt_gu

[2] https://www.extremetech.com/internet/255311-equifax-fine-print-keeps-getting-longer-situation-mostly-gets-worse?utm_source=email&utm_campaign=dailynews&utm_medium=image

[3] https://www.heise.de/forum/heise-online/News-Kommentare/Hacker-Jackpot-Credit-Bureau-Equifax-gehackt/forum-387653/comment/

zertifizierte Anbieter und deren Rechenzentren bieten: unterbrechungsfreie Stromversorgung, aufwendige Vorkehrungen für Brandschutz sowie Backup-Lösungen an verteilten Standorten. Unerwähnt bleiben sollte in diesem Zusammenhang auch nicht eine stets aktuelle Firewall und die neuesten Verschlüsselungs-Technologien.

54 % der befragten Unternehmen halten ihre eigenen Sicherheitsstrategien laut der „2016 Global Cloud Data Security Study“ für nicht ausreichend[4]. Die Unternehmen leben mit der nicht unbegründeten Befürchtung, dass sensible Daten zu sorglos mit Geschäftspartnern oder Kunden geteilt werden. Erschwerend kommt hinzu, dass fast die Hälfte aller Daten in der Cloud nicht von der IT-Abteilung verwaltet und kontrolliert wird, sondern von anderen Abteilungen im Unternehmen. Bitkom Research kommt zu ähnlichen Zahlen: Nach der repräsentative Umfrage „Cloud Monitor 2017“ stieg die Anzahl der Cloud-Nutzer im Jahr 2016 auf 65 % – eine Steigerung von 11 % im Vergleich zum Vorjahr[5]. 24 % der Unternehmen planen oder prüfen einen zukünftigen Wechsel in die Cloud. Eine Vorreiterrolle nehmen dabei Unternehmen der chemisch-pharmazeutischen Industrie ein: 88 % von ihnen nutzen bereits Cloud-Dienste wie Software-as-a-Service (SaaS).

Dr. Axel Pols, Geschäftsführer von Bitkom Research, resümierte die Ergebnisse: „Cloud-Computing hat sich durchgesetzt und innerhalb weniger Jahre zur Basis-Technologie der Digitalisierung entwickelt. Die bedarfsgerechte Nutzung von IT-Leistungen über Datennetze bietet enorme Vorteile“.

2.3 Wahl des Providers

Doch Cloud ist nicht gleich Cloud: Die wichtigsten Unterscheidungsmerkmale bestehen in den Standorten der Rechenzentren, in der Kontrolle über den Datenfluss und in Form der angebotenen Services. Der Standort ist entscheidend, weil unterschiedliche Länder unterschiedliche Datenschutz-Gesetze anwenden. Spätestens seit den Enthüllungen von Edward Snowden ist bekannt, dass die großen externen Rechenzentren von Microsoft und Google nicht so sicher sind wie versprochen[6] sind. Amerikanische Behörden haben bestätigt, dass der europäische Datenschutz nicht für US-Firmen gilt, die in Europa tätig sind. Anwendersoftware amerikanischer Unternehmen wie Microsoft OneDrive for Business, Dropbox Business oder Box Business unterliegen dem US-Recht, was zur Folge hat, das gespeicherte personen- und unternehmensrelevante Daten unabhängig vom Standort der Server nicht vor dem Zugriff von US-Behörden geschützt sind. Wer sichergehen will, wählt deshalb einen Anbieter, dessen Server im Inland stehen. TeamDrive-Kundendaten werden ausschließlich in deutschen Rechenzentren gespeichert.

Wer als Anwender darüber nachdenkt, Services aus der Cloud zu nutzen, sollte die Angebote sorgfältig prüfen. Dazu zählt vor allem, die Herkunft des Anbieters und der Standort des Cloud-Servers. Befinden sich der Hauptsitz des Anbieters und das Rechenzentrum in Deutschland, unterliegt die Cloud dem deutschen Datenschutz und der deutschen Rechtsprechung.

2.4 Ausgezeichnete Sicherheit

Cloud-Computing ist Vertrauenssache. Zertifizierungen bieten eine Orientierung für ein Sicherheits- und Qualitätsmanagement des Dienstleisters. Zertifikate belegen, dass ein Cloud-Dienstleister bestimmte Datenschutzrichtlinien einhält.

Beispielsweise hat der Deutsche Anwaltverein e. V. zusammen mit der TeamDrive Systems GmbH eine spezielle Cloud-Datenspeicherlösung für Anwälte definiert. Mit einer Ende-zu-Ende-Verschlüsselung und garantierten Sicherheitsstandards beim Server-Hosting empfiehlt der Deutsche Anwaltverein e. V. seinen rund 68.000 Mitgliedern die moderne Lösung für das Speichern, Synchronisieren und Teilen von Daten und Dokumenten, die den besonderen Anforderungen des Berufsstandes als Geheimnisträger nach § 203 StGB und BDSG gerecht wird. Kanzleien und Anwälte haben die Gewissheit, beim Speichern, Synchronisieren und

[4] https://safenet.gemalto.com/resources/data-protection/cloud-security-study-2016-report/

[5] https://www.bitkom.org/Presse/Anhaenge-an-PIs/2017/03-Maerz/Bitkom-KPMG-Charts-PK-Cloud-Monitor-14032017.pdf

[6] http://www.sueddeutsche.de/digital/internet-ueberwachung-snowden-macht-das-internet-sicherer-1.1984638

Teilen von Daten und Dokumenten nicht unfreiwillig die Interessen ihrer Klienten zu verletzen. Durch die Verwendung von TeamDrive ist es jederzeit gewährleistet, dass die vertraulichen Daten ausschließlich verschlüsselt übertragen und unter genau festgelegten Bedingungen in einem dedizierten Hochsicherheitsrechenzentrum in Deutschland gespeichert sind.

Die Software TeamDrive ist gemäß § 4 Abs. 2 LDSG i. V. m. der Datenschutzauditverordnung (DSAVO) mit dem Datenschutzgütesiegel des Landeszentrums für Datenschutz Schleswig-Holstein ausgezeichnet.

Die mehrfach ausgezeichneten Rechenzentren sind nach ISO/IEC 20000-1 und nach ISO 27001 nach dem IT- Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zertifiziert.

Die Gartner Inc., eines der weltweit größten IT-Beratungs- und Analystenhäuser, hat TeamDrive in die Liste der "Cool Vendor for Privacy 2013" aufgenommen.

2.5 Vertrauen ist gut, Kontrolle ist besser

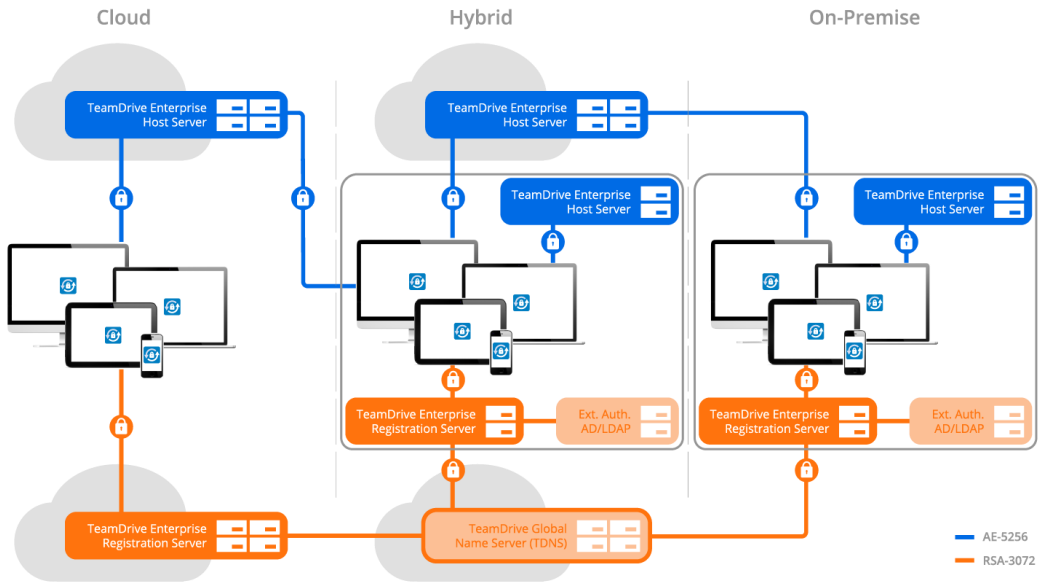
Die Punkte Datenschutz und Datensicherheit zählen bei der Auswahl des Cloud-Modells zu den entscheidenden Kriterien. Datenspeicherung ist Vertrauenssache: Im Gegensatz zu intransparenten Public-Cloud-Lösungen wie Box, Dropbox, Microsoft OneDrive bietet die TeamDrive Systems ihren Kunden eine vollwertige Ende-zu-Ende-Verschlüsselung (AES 256-Bit) für ihre Daten und Dokumente mit einer Speicherung in dedizierten Rechenzentren am Standort Deutschland (Private-Cloud).

Vor allem Branchen, die mit einer großen Menge sensibler Daten umgehen müssen, greifen bisher auf das bewährte Modell der Privat-Cloud zurück. In der Privat-Cloud hat der Anwender die entsprechende IT- Umgebung für sich allein. Die Private-Cloud wird entweder im eigenen Rechenzentrum aufgebaut oder sie befindet sich beim Dienstleister – aber getrennt von denen der anderen Kunden.

In den letzten Jahren hat sich die „Hybrid-Cloud[7]“ als verbreitetes und zukunftsorientiertes Modell herauskristallisiert. Als „Hybrid-Cloud“ wird eine Cloud-Umgebung bezeichnet, in der Unternehmen einen Teil ihrer IT-Ressourcen vor Ort (On-Premise) verwalten, während der andere Datenanteil bei einem Service-Provider gehostet wird.
TeamDrive unterstützt die Benutzung einer hybriden Cloud und bietet Ihnen anders als Box, Dropbox oder Microsoft OneDrive nicht nur Cloud-Services sondern eine freie Serverwahl an: Sie können Ihre Daten ausschließlich bei von TeamDrive gehosteten Servern, auf Ihren eigenen Servern oder auf Servern eines von Ihnen gewählten Dienstleisters speichern. Der TeamDrive Sicherheits-Layer bietet Ihnen einen Schutz über die vorhandene Infrastruktur Ihres Unternehmens.

[7] https://digitales-wirtschaftswunder.de/Crisp-QSC-Multi-Cloud-Studie.pdf

Abbildung 1: Verwendung einer Hybrid-Cloud mit TeamDrive



3 DSGVO-Countdown

3.1 Folgen des Inkrafttretens des DSGVO

Künftig haben natürliche Personen einen einfacheren Zugang zu ihren Daten. Jede natürliche Person hat damit das Recht zu erfahren, welche Daten über sie gesammelt und gespeichert werden. Außerdem hat jede natürliche Person einen Anspruch auf einfach verständliche Informationen, wer ihre Daten zu welchem Zweck verwendet bzw. weiterverarbeitet.

Dazu gehört auch, dass eine natürliche Person zukünftig noch ausführlicher darüber informiert werden muss, wenn ihre Daten unbefugt entwendet wurden. Damit soll es jeder natürlichen Person zeitnah möglich sein, Maßnahmen zu ihrem Schutz zu ergreifen.

Personenbezogene Daten gehören stets der jeweiligen natürlichen Person und nicht einem mit der Datenverarbeitung befassten Internetdienst.

Mit der neuen DSGVO wird jede natürliche Person das Recht haben, ihre Daten von einem Internetanbieter zum anderen mitzunehmen. Zudem wird das „Recht auf das Vergessen“ veröffentlichter Informationen über eine natürliche Person gestärkt, indem der natürlichen Person das Recht zugesprochen wird, einmal über sie veröffentlichte Informationen löschen zu lassen.

TeamDrive als deutsches Unternehmen bietet gegenüber Box, Dropbox, Microsoft OneDrive, Google Drive oder Amazon AWS entscheidende Vorteile, da TeamDrive für seine europäischen Kunden ausschließlich Rechenzentren in Deutschland zur Datenspeicherung in Europa nutzt. Ihre Daten unterliegen den Datenschutzbestimmungen gemäß Bundesdatenschutzgesetz (BDSG). Die automatische Speicherplatzzuweisung während der Anmeldung basiert auf der IP-Adresse bei der Registrierung. Die Server-Zuordnung ändert sich nicht während der Laufzeit der Nutzung, unabhängig von wo aus Sie den Service in Anspruch nehmen.

3.2 Was bedeutet das konkret für Ihr Unternehmen?

Der §9 BDSG schreibt vor, das „öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, die technischen und organisatorischen Maßnahmen zu treffen haben, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten haben.“

Die genannte Anlage zu §9 BDSG verlangt, dass der Zutritt, der Zugang, der Zugriff und die Weitergabe personenbezogener Daten kontrolliert werden. Kontrollbedürftig ist darüber hinaus, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt werden. Schlussendlich ist zu gewährleisten, dass personenbezogene Daten

- nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können
- gegen zufällige Zerstörung oder Verlust geschützt sind und
- dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Die Verwendung von dem Stand der Technik entsprechender Verschlüsselungsverfahren wird explizit empfohlen.

3.3 Das IT-Sicherheitsgesetz (ITSiG)

2014 präzisierte Bundesinnenminister Thomas de Maizière in der Frankfurter Allgemeinen Zeitung (FAZ): „Wer durch den Einsatz von IT Risiken für andere schafft, hat auch die Verantwortung für den Schutz vor diesen Risiken.“[8] Je schwerwiegender die Risiken, desto höher müssten die Anforderungen an Schutzvorkehrungen sein. Weiter schrieb de Maizière: „Auf freiwilliger Basis bestehende Angebote und Initiativen in Anspruch zu nehmen reicht hier nicht mehr aus!“ Der Staat müsse deshalb „Sicherheitsgurte für

[8] http://www.faz.net/aktuell/politik/inland/de-maiziere-ueber-die-digitale-agenda-deutschland-wird-it-vorreiter-13103217.html

die IT der kritischen Infrastrukturen“ einführen.
Die Ziele von EU und Bundesregierung nennt das BSI: „Widerstandsfähigkeit ("Resilience") gegenüber Cyberangriffen:

1. Drastische Eindämmung der Cyberkriminalität
2. Entwicklung einer Cyberverteidigungspolitik und von Cyberverteidigungskapazitäten im Zusammenhang mit der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP)
3. Entwicklung der industriellen und technischen Ressourcen für die Cybersicherheit
4. Entwicklung einer einheitlichen Cyberraumstrategie der EU auf internationaler Ebene und Förderung der Grundwerte der EU.

In der FAZ kündigte de Maizière auch das IT-Sicherheitsgesetz an – neben dem Gesundheitswesen werden darin auch die Bereiche Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Wasser, Ernährung sowie das Finanz- und Versicherungswesen als „kritische Infrastrukturen“ bezeichnet.
Besonders verantwortungsbewusst wäre es in diesem Zusammenhang, wenn die Anbieter die technischen und organisatorischen Maßnahmen schon getroffen hätten, noch bevor diese vom Gesetzgeber gefordert wurden.

3.4 Drakonische Strafen bei Verstößen gegen die EU - DSGVO

Die Europäische Datenschutzgrundverordnung tritt ab dem 25. Mai 2018 in Kraft. Ab diesem Zeitpunkt sind Unternehmen verpflichtet, ein Datenschutzmanagement einzuführen, um personenbezogene Daten zu sichern.

Bislang wurden Verstöße gegen das DSGVO oftmals wie Kavaliersdelikte behandelt und entsprechend lax bestraft. Damit soll künftig Schluss sein: In Artikel 83 sind „Allgemeine Bedingungen für die Verhängung von Geldbußen“ definiert: „Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sind.“ Im Klartext heißt das: „Bußgelder müssen nach den neuen Regelungen in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sein.“
Jeder, der geschäftsmäßig mit personenbezogenen Daten Dritter umgeht, tun gut daran, sich mit den neuen Vorschriften auseinanderzusetzen und sich darauf einzustellen, was in Zukunft gelten wird, um einen kräftigen Bußgeldbescheid zu vermeiden.“
Das Ziel lautet: Die „Sicherheit der Verarbeitung“ (Artikel 32) – auch durch Dritte: Der Verantwortliche und der Auftragsverarbeiter sollen durch geeignete technische und organisatorische Maßnahmen ein „dem Risiko angemessenes Schutzniveau“ bieten. Dabei sollen der Stand der Technik sowie Art, Umfang, Umstände und Zweck der Verarbeitung sowie Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen berücksichtigt werden“. Im Klartext bedeutet das: Kommen personenbezogene Daten abhanden, ist das der Aufsichtsbehörde innerhalb von 72 Stunden zu melden. Zudem ist der betroffene Personenkreis unverzüglich über den Datenverlust zu informieren, es sei denn, mit dem Verlust der Daten ist kein hohes Risiko verbunden. Das ist der Fall, wenn die Daten nach dem Stand der Technik verschlüsselt sind.

Gemäß Artikel 33 DSGVO müssen die zuständige Aufsichtsbehörde sowie die betroffenen Personen (Artikel 34 DSGVO) unverzüglich verständigt werden, spätestens aber innerhalb von 72 Stunden nach Bekanntwerden einer Verletzung.

Gemäß Artikel 34.3 (a) sind Sie bei einer Verletzung des Schutzes personenbezogener Daten, die voraussichtlich ein hohes Risiko für die Rechte natürlicher Personen zur Folge hat, nicht zur Meldung des Vorfalls verpflichtet, wenn diese Daten verschlüsselt waren. Mit der Verwendung von TeamDrive ist dieser Schutz gewährleistet.

Die Höhe der Bußgelder ist drakonisch: Wer gegen die Verordnung verstößt, riskiert gemäß Artikel 83 nicht nur eine Geldbuße, die, wie es im Gesetz heißt „in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist“ – das heißt „bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes“ betragen kann: „je nachdem, welcher der Beträge höher ist“. Wichtig zu wissen ist: Der Gesamtverband der Deutschen Versicherungswirtschaft schließt Versicherungen gegen Geldbußen aus – wegen befürchteter „Sittenwidrigkeit“. Das heißt: Die Zeche zahlt der Verantwortliche persönlich! Es sind darüber hinaus Schadenersatzansprüche für die Erwähnten materiellen und immateriellen Schäden möglich (Artikel 82). Die DSGVO sieht ein Verbandsklagerecht (Artikel 80) vor. Dabei „haftet jeder Verantwortliche oder jeder Auftragsverarbeiter für den gesamten Schaden, damit ein wirksamer Schadensersatz für die betroffene Person sichergestellt ist“. Darüber hinaus ist die Aufsichtsbehörde befugt, die Datenverarbeitung zu verbieten (Artikel 58). Eine ebenfalls schlimme Strafe stellt der Image-Verlust dar: Ist ein Unternehmen vermehrt Opfer von Cyber-Angriffen, sinkt das Vertrauen in den Anbieter. Etwa jeder Dritte ist bereit, unter diesen Umständen ein Produkt oder eine Marke zu wechseln.

Sicherheitslücken und Datenangriffe einerseits, Geldbußen und Schadenersatzforderungen andererseits werden zur existentiellen Bedrohung – die Organisation für wirtschaftliche Zusammenarbeit OECD warnte 2016: Die bezüglich Qualität, Quantität und Heftigkeit wachsenden Datenangriffe könnten die Fähigkeit eines Mittelständlers zur Innovation untergraben und seine Marktposition schwächen. Wer nicht die finanziellen Mittel hat, um die Rechtsberatung, forensische Untersuchungen, die vorgeschriebenen Benachrichtigungen, die Wiederherstellungsmaßnahmen, die Geldbußen und Gerichtsurteile zu bezahlen, könne schnell aus dem Markt ausscheiden.

Laut einer Studie des Dienstleisters Veritas[9] sollen weniger als zehn Prozent der Unternehmen ab 1000 Mitarbeitern die Verordnung zum jetzigen Zeitpunkt umgesetzt haben. Unter Umständen hängt das damit zusammen, dass bei Unternehmen ein mangelhaftes Verständnis für das Konzept des Stands der Technik vorliegt. Der Mangel an Verständnis der für die Informationssicherheit Verantwortlichen Chefs ist das Eine noch schlimmer wirkt sich allerdings aus, dass der Mangel an Sicherheits-Fachkräften nach Erkenntnis der Marktforschungsfirma Frost & Sullivan bis 2022 um 20 Prozent gegenüber 2015 erhöhen soll[10]. Darunter werde insbesondere der Mittelstand zu leiden haben.

Die Zeit bis Mai 2018 drängt; insbesondere für kleine Unternehmen: Unternehmen mit weniger als zehn Mitarbeitern mussten bislang nicht einmal einen Datenschutzbeauftragten beschäftigen (§4e BDSG (Bundesdatenschutzgesetz)). Es ist nicht auszuschließen, dass Kleinunternehmen bis heute noch nicht einmal über ein Verfahrensverzeichnis verfügen (§4d BDSG). Somit ist die Frage begründet, wie kleine Unternehmen die Vorgaben der Informationssicherheit bis Mai 2018 umsetzen wollen. Es scheint beinahe unmöglich, je näher der 25. Mai 2018 (der Tag, ab dem die DSGVO von den Unternehmen anzuwenden ist) rückt, desto schwieriger dürfte es für diese Unternehmer werden, überhaupt einen Berater zu finden, der sie beim Umsetzen der gesetzlichen Forderungen unterstützt.

Neben einer Geldbuße könnten Ansprüche aus Schadenersatzforderungen hinzukommen. Artikel 82 der Verordnung besagt: „Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.“

3.5 Großer Nachholbedarf für IT-Sicherheit und Datenschutz

„Alles, was digitalisiert werden kann, wird digitalisiert. Und alles, was vernetzt werden kann, wird vernetzt“, ist Telekom-CEO Timotheus Höttges[11] überzeugt. Neben Kommunikation und Prozessen lassen sich auch

[9] Veritas: Schlusslicht Deutschland: Unternehmen fühlen sich schlecht auf DSGVO vorbereitet, 25.4.17, https://www.veritas.com/de/de/news-releases/2017-04-25-veritas-study-organizations-worldwidefear-non-compliance-with-new-european-union-data-regulation-could-put-them-out-of-business

[10] https://www.computerwoche.de/a/grosser-mangel-an-it-sicherheitsfachkraeften,3331095

[11] https://www.heise.de/newsticker/meldung/Telekom-Chef-Alles-wird-vernetzt-2661572.html

Verbrauchsgegenstände digitalisieren: Verbrauchsmaterial wird bei Verminderung des Bestands automatisch nachgebucht, Smart Metering-Komponenten können aus der Ferne gesteuert und ausgewertet werden, Fahrzeuge können per App geortet und angemietet werden usw. Eine wachsende Vernetzung ist die Konsequenz des „Internet der Dinge“: Zulieferer vernetzen sich mit Herstellern und Händlern, Krankenhäuser und Arztpraxen mit Krankenkassen, Architekten mit Ingenieuren, Bauämtern, und Immobilienverwaltungen. Das ermöglicht eine „Wirtschaft in Echtzeit“. Allerdings ist nicht jeder, der an Informationen herankommt, auch dazu berechtigt: So sollen einer Studie des Speicherherstellers Kingston zufolge 95 % der Firmen ihre Unternehmensdaten auf USB-Geräten speichern, mehr als die Hälfte davon unverschlüsselt[12]. Und 39 % der Beschäftigten sollen diese Speicher bereits mindestens einmal verloren haben. Mehr als die Hälfte der befragten Firmen soll die Daten auf ihren mobilen Speicher nur „unzureichend“ gesichert haben.

Nur vier von zehn Mittelständlern verschlüsseln Daten und Festplatten. In 40 % der Unternehmen sollen die Mitarbeiter Sicherheitspannen verheimlichen, wie der Hersteller der Antivirus-Software Kaspersky herausgefunden haben will. Das wird im Unternehmensnetz nicht besser: 33 % der Unternehmen sollen nicht einmal wissen, wo ihre Daten physikalisch gespeichert sind.

Zwar sollen 55 % der Unternehmen weltweit nach Erkenntnis von Gartner über ein „Identity und Access Management“-System verfügen. Das würde allerdings auch bedeuten: 45 % der Unternehmen wissen nicht, wer Zugang zu welchen Informationen hat. Dirk Kretzschmar, Geschäftsführer der TÜV Informationstechnik (TÜViT) glaubt, dass nur 3 % der Unternehmen auf Datenangriffe vorbereitet seien. Risikoexperten warnen gleichzeitig, ein starkes Cyber-Sicherheitsprogramm sei „überlebenswichtig“ im Computerzeitalter.

3.6 DSGVO verlangt Nachweis der Datensicherheit

Zur Vermeidung von Cyber-Angriffen gilt in der Europäischen Union ab dem 25. Mai 2018 die Datenschutzgrundverordnung (DSGVO). Behörden und Unternehmen müssen in der Lage sein, die Sicherheit ihrer Datenverarbeitung jederzeit nachzuweisen: Dazu sollte der Verantwortliche gemäß Erwägungsgrund 78 der Verordnung "interne Strategien festlegen und Maßnahmen ergreifen, die insbesondere den Grundsätzen des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) Genüge tun". Der Verantwortliche könnte sich diesen Nachweis gemäß Artikel 42 am einfachsten durch ein entsprechendes Zertifikat bescheinigen lassen. TeamDrive erfüllt diese Ansprüche bereits zum jetzigen Zeitpunkt: TeamDrive liefert mit dem Datenschutzsiegel einer behördennahen Institution den Qualitätsnachweis für Datensicherheit.

Die DSGVO verlangt gemäß Artikel 32: „Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“.

Zu diesen Risiken zählt die Verordnung (Erwägungsgrund 75) auch physische, materielle oder immaterielle Schäden, Identitätsdiebstahl oder -betrug, finanzielle Verluste, Rufschädigung, wirtschaftliche oder gesellschaftliche Nachteile. In diesem Zusammenhang ist die mögliche Sabotage durch Innentäter – oder das Eindringen von Schadsoftware zu berücksichtigen. Diese Gefahren wollen erfasst und bewertet werden. Für den dadurch erforderlichen Prozess empfiehlt das Bundesamt für Sicherheit in der Informationstechnik (BSI) seinen Risikomanagement-Standard 200-1.

3.7 DSGVO fordert Sicherheit nach dem Stand der Technik

„Stand der Technik ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen und Betriebsweisen,

[12] http://www.kingston.com/de/company/press/article/48111

der nach herrschender Auffassung führender Fachleute das Erreichen des gesetzlich vorgegebenen Zieles gesichert erscheinen lässt.“ Technik und Verfahren müssten sich „in der Praxis bewährt haben“ oder – wenn dies noch nicht der Fall sei - „möglichst im Betrieb mit Erfolg erprobt worden sein“, definieren Anwälte und Informatiker vom TeleTrusT-Bundesverband IT-Sicherheit e. V. den Begriff[13]. Im Recht der Europäischen Union werde auch die Formulierung „die besten verfügbaren Techniken“ verwendet. Diese entsprächen nach Ansicht der Autoren weitgehend der Generalklausel "Stand der Technik".

3.8 Sicherheit ist kein Hindernis für die Cloud-Nutzung

Wenn über solche Wege Daten übertragen werden, spielt das Thema Sicherheit eine große Rolle. Schließlich handelt es sich bei personenbezogenen Daten um sensible Informationen. Nur wenige Unternehmen sehen Cloud-Lösungen noch als Hindernis, Technik in der Cloud zu nutzen. Vor wenigen Jahren gab es bei dem einen oder anderen Kunden noch Bedenken hinsichtlich Cloud Computing, vor allem aus Gründen der Sicherheit. Das hat sich mittlerweile geändert: Cloud-Computing hat sich als Technologie inzwischen etabliert. Kunden erkennen mittlerweile die Vorteile bei der Verwendung eines Public-Cloud-Anbieters im Vergleich zum klassischen On Premise-Hosting. Hierbei gelten die hohen Sicherheitsstandards in Deutschland als das Maß der Dinge.

Ein Cloud-Anbieter kann die Datensicherheit besser gewährleisten, als es Anwenderunternehmen in der Regel selbst können. Gerade klein- und mittelständigen Unternehmen sind mit den Anforderungen einer sicheren Datenhaltung häufig überfordert.

3.9 Deutschland in puncto Sicherheit als beliebter Standort für Rechenzentren

Zahlreiche Kunden legen großen Wert darauf, dass ihre Daten in Deutschland verbleiben und hier gehostet werden. In Deutschland gehostete Daten müssen die Datenschutz- und Sicherheitsstandards gemäß deutschem Recht erfüllen. Daten und Dokumente, die unter Verwendung von der TeamDrive-Software lokal und auf Servern gespeichert werden, sind zu jedem Zeitpunkt Ende-zu-Ende verschlüsselt (AES 256-bit). Das bedeutet, das mit TeamDrive bearbeitete und synchronisierte Daten und Dokumente nach heutigem Stand der Technik von niemandem zu keinem Zeitpunkt eingesehen werden können.

[13] https://www.teletrust.de/publikationen/broschueren/stand-der-technik/

4 Sync&Share-Software TeamDrive

4.1 Über TeamDrive

TeamDrive ist eine Sync- und Kollaborationslösung für multiple Einsatzgebiete. Sync- und Kollaborationslösungen unterstützen die Zusammenarbeit von Teams bei der Kommunikation, der Erstellung und Archivierung von Dokumenten.

TeamDrive bietet Benutzern und Benutzergruppen die Möglichkeit, auf einen gemeinsamen Datenbestand zuzugreifen und Änderungen an Dokumenten auszuführen. Der Datenbestand ist in TeamDrive zu jedem Zeitpunkt Ende zu Ende-verschlüsselt (AES 256-Bit) und schützt Ihre Daten und Dokumente vor dem unberechtigten Zugriff Dritter.

Mit TeamDrive können Benutzer projektbezogene Daten und Dokumente mit Kollegen, Kunden, externen Dienstleistern und Partnern teilen. In TeamDrive heißt ein gemeinsam verwendeter Arbeitsbereich „Space“. Ein „Space“ entspricht einem Ordner im Dateisystem. In einem „Space“ können Sie beliebig viele Ordner, Unterordner und Dateien speichern. Dateien und Dokumente können per Drag-and-drop einem „Space“ in Teamdrive oder einem Ordner im Dateisystem hinzugefügt werden.

Über ein Berechtigungskonzept legen Sie fest, wer in einem Space welche Aktionen ausführen darf. Ein Administrator eines Space verwaltet die Mitglieder eines Teams. Als Administrator eines Space laden Sie Kollegen oder Partner per E-Mail in einen Space ein und erlauben somit den zuvor definierten Zugriff auf Dateien und Ordner. Optional können Sie einen Ordner aus Ihrem Dateisystem in einen Space ändern und in TeamDrive verwalten. Sie können in TeamDrive auch auf Dateisystemebene arbeiten. Es ist ebenfalls möglich, über ein Browser-Interface (Web-Client) auf Ihren Datenbestand zuzugreifen.

Ein Space wird auf einem TeamDrive Hosting-Server, der in der TeamDrive-Cloud, auf einem WebDAV-Server oder On-Premise auf einem Server bei Ihnen im Unternehmen gespeichert.

TeamDrive überwacht beliebige viele lokale Dateien und Ordner im Dateisystem und in Spaces und synchronisiert diese mit den persönlich eingeladenen Team-Mitgliedern. TeamDrive ist geeignet für die Synchronisierung von Dateien und Ordnern zwischen mehreren Computern oder mobilen Endgeräten. Sämtliche Dateien und Dokumente stehen allen Team-Mitgliedern jederzeit - auch offline - im Dateisystem zur Verfügung. Durch die Server-Kommunikationsstruktur von TeamDrive werden die Daten standardmäßig zwischen den verwendeten Computern und mobilen Endgeräten automatisch synchronisiert (diese Standard-Einstellung kann bei Bedarf deaktiviert werden). TeamDrive verwendet hierbei verschiedene Vermittlungsserver, um eine Verfügbarkeit für Teams und deren Mitglieder sicherzustellen. Der Datenbestand ist in TeamDrive auf dem Transportweg zwischen Ihrem Computer und dem Server zu jedem Zeitpunkt Ende zu Ende-verschlüsselt (AES 256-Bit) und Stand der Technik vor dem unberechtigten Zugriff Dritter geschützt.

Aufgrund seiner Datensicherheit eignet sich TeamDrive besonders für Unternehmen und Berufsgruppen, die sensible Daten vorhalten, wie beispielsweise Banken und Versicherungen, Universitäten, Rechtsanwälte, Notare oder Mitarbeiter aus der Medizin sowie der Forschung und Entwicklung.

Als Vermittlungsserver können Sie entweder die sichere Cloud, eigene Server oder einen kompatiblen WebDAV-Server verwenden. Die Software TeamDrive Personal Server kann ebenfalls für diesen Zweck verwendet werden. Optional können Sie Dienstangebote kommerzieller Provider nutzen.

TeamDrive steht für die Betriebssysteme MS Windows, Mac OS X/macOS, Linux, iOS Android und als Web-Client zur Verfügung.

4.2 Audit-Trail

Ein Audit-Trail ist eine chronologische Abfolge von Handlungen, Ereignissen oder Systemzuständen, die durch Spuren dokumentiert und damit zurückverfolgt werden können. Ein Audit-Trail dient der Prüfung bzw. Überwachung der Handelnden und ihrer Aktivitäten.

Mit dem integrierten Audit-Trail werden geänderte Daten in TeamDrive protokolliert und können ausgewertet werden. Das integrierte Audit Trail ermöglicht eine detaillierte, durchgängige und nachvollziehbare Beschreibung alle Veränderungen von Daten und Dokumenten in TeamDrive.

Jede Änderung von Daten im System werden in eine Transaktions-Logdatei geschrieben. Wird eine Datei erzeugt, wird ein Eintrag mit der Global ID des Dokuments mit Datum und Zeitstempel, User-ID und Device-ID der Transaktions-Logdatei hinzugefügt. Auch Änderungen wie z. B. Umbenennen, Verschieben, das Erstellen einer neuen Dokumentenversion oder das Löschen eines Dokuments werden unter Angabe des Benutzers (User-ID) und des verwendeten Computers bzw. mobilen Endgeräts (Device-ID) im Transaktionslog gespeichert.

Zusätzlich werden alle Information über den Benutzer und seine Rechte gespeichert:

- wann wurde ein Benutzer mit welchen Rechten eingeladen?
- wann hat ein Benutzer die Einladung angenommen?
- wann hat ein Benutzer auf welche Daten bzw. auf welches Dokument zugegriffen?
- mit welchem Device hat ein Benutzer zugegriffen?

Eine Auswertung des Audit Trail kann als CSV-Datei exportiert werden.

Die Audit Trail Exportdatei ist mit AES 256-Bit verschlüsselt; somit ist eine nachträgliche Bearbeitung oder Manipulation der Exportdatei nicht möglich. Die Transaktions-Logdatei wird auf dem TeamDrive Hosting Server gespeichert und kann vom Benutzer nicht geändert werden.

4.3 Point in Time Recovery

Ein Leistungsmerkmal von TeamDrive ist eine Snapshot-Technologie. Point in Time Recovery ist eine Technologie zur Datensicherung und -wiederherstellung eines Datenabbilds (Snapshot). Teamdrive erstellt automatisch in regelmäßigen Abständen (auf Wunsch alle 30 Minuten) einen Snapshot des aktuellen Datenbestandes für alle von einem Benutzer verwendeten Computer. In beiden Fällen können Daten bei einem Datenverlust (z. B. durch einen Hardware-Defekt oder einen Ransomware-Angriff) mit wenigen Handgriffen vollständig wiederhergestellt werden. In der Privatkunden-Version werden die gesicherten Daten nach 30 Tagen gelöscht. Die Version für den professionellen Betrieb erlaubt Aufbewahrungszeiten von bis zu zehn Jahren, um beispielsweise gesetzlichen Vorgaben oder vertraglichen Regelungen zu genügen.

5 Schutzmaßnahmen

5.1 Versionskontrolle

In TeamDrive werden alle Daten - einschließlich früherer Versionen - inklusive der Metadaten auf einem Server gespeichert.

Durch die automatische Versionskontrolle kann zu jedem Zeitpunkt auf die aktuelle Version eines Dokuments zugegriffen werden. Zu jeder Version eines Dokuments werden detaillierte Informationen zum Autor, zur Version, zur Vorversion und zum Datum der letzten Änderung gespeichert. In der Versionsübersicht können alle Versionen eines Dokuments angezeigt und Konflikte zwischen unterschiedlichen Versionen gelöst werden.

Daten werden innerhalb des TeamDrive-Netzwerk zu keinem Zeitpunkt unverschlüsselt übertragen. Alle Dokumente werden auf dem Server verschlüsselt, bevor sie gespeichert und versendet werden. Eine Entschlüsselung von Daten ist nur durch Mitglieder in einem Space möglich.

5.2 Sicherheit

Gespeicherte Daten auf Ihrem Computer sind in der Regel unverschlüsselt. Alle Daten, die Sie in TeamDrive speichern und versenden, sind AES 256 Bit verschlüsselt. Um die Sicherheit zusätzlich zu erhöhen, kann TeamDrive auf einer verschlüsselten Partition (z. B. auf einem mit VeraCrypt- oder PGP-verschlüsselten Datenträger) installiert und verwendet werden.

Tabelle 1: Schnellübersicht der wichtigsten Funktionalitäten

TeamDrive in der Übersicht	Beschreibung
Ortsunabhängig, flexibel und schnell	Nutzen Sie TeamDrive ortsunabhängig auf Ihrem Laptop, Tablet oder Smartphone. Partner oder Dienstleister können von überall auf einen Spaces zugreifen, wenn Sie Teammitglied sind.
Betriebssysteme	MS Windows, Mac OS X/macOS, Linux, iOS, Android (optional kann der TeamDrive mit jedem handelsüblichen Browser verwendet werden).
Verschlüsselung	Jeder Space verfügt über einen eigenen sicheren AES 256-Bit Schlüssel (die Schlüssel verbleiben immer auf Ihrem Rechner)
Passwort und Ablaufdatum	Sie können Dateien mit einem Passwort und/oder Ablaufdatum versehen.
Verschlüsselung	Jeder Space hat einen eigenen sicheren AES 256-Bit Schlüssel (die Schlüssel verbleiben immer auf Ihrem Rechner)
Individuelles Berechtigungskonzept	Der Ersteller eines Space ist auch der Administrator des Space. Individuelle Vergabe von Benutzerrechten je Space.

TeamDrive in der Übersicht	Beschreibung
Teamarbeit	Einrichten von Teams, um gemeinsam an Dokumenten zu arbeiten.
Point-in Time-Recovery	Einfache Datenwiederherstellung aus einem Snapshot, z. B. bei einem Virusbefall.
Hybrid Cloud	Zeitgleiche Verwendung unterschiedlicher Server-Typen: On-Premise, WebDAV, Cloud-Computing oder als Kombination.
Versionsverwaltung	Automatische Versionsverwaltung für alle Dokumente.
Backup	Automatische Backup-Funktion Ihrer Daten.
Dokumentenbearbeitung	Offline-Bearbeitung mit automatischer Synchronisation.
Synchronisation	Synchronisation von beliebig vielen Ordnern und Dokumenten (im Rahmen des verfügbaren Server-Speicherplatzes).
Benachrichtigungszentrum	Sie erhalten Benachrichtigungen über neue Versionen, Kommentare, Einladungen, Konflikte, Fehler usw.
Dateiformate	Unterstützung beliebiger Dateiformate für Dokumente, Bilder, Videos oder Programme.

6 Glossar

AES-Verschlüsselung

Unter AES-Verschlüsselung versteht man eine Ende-zu-Ende-Verschlüsselung übertragener Daten über alle Übertragungsstationen hinweg. Die zu übertragenden Daten werden auf Senderseite verschlüsselt und erst beim Empfänger wieder entschlüsselt. Die Bezeichnungen der AES-Varianten beziehen sich auf die gewählte Schlüssellänge. Je höher der AES-Wert, desto höher ist der Verschlüsselungsgrad. TeamDrive verwendet die derzeit höchste Verschlüsselungsstufe mit AES 256-Bit.

Audit Trail

Audit-Trail ist ein softwarebasiertes Verfahren in Betriebssystemen, Datenbanksystemen oder in Anwender- und Verwaltungssoftware, bei dem Benutzer und ihre Aktivitäten über einen definierten Zeitraum überwacht und protokolliert werden. Das Verfahren dient einerseits der Überwachung der Benutzeraktivitäten, anderseits kann durch Audit-Trail eine System- bzw. Datenwiederherstellung im Fehlerfall vereinfacht werden.

CSV-Datei

Mit der Abkürzung CSV (engl. für comma separated values, dt. kommaseparierte Werte) wird bei der Datenverarbeitung ein Textdateityp bezeichnet, mit dessen Hilfe auch große Mengen an strukturierten Daten erfasst, gespeichert und verarbeitet werden können.

Cloud

Cloud bzw. Cloud Computing beschreibt eine Bereitstellung einer IT-Infrastruktur wie z. B. Speicherplatz, Rechnerleistung oder Anwendersoftware als Dienstleistung über das Internet. Die TeamDrive Systems GmbH stellt diese Art von Dienstleistung zur Verfügung. Die von der TeamDrive Systems GmbH verwendeten Server für europäische Benutzer befinden sich in Deutschland und unterliegen den deutschen Datenschutzrichtlinien.

Host

Ein Host ist ein im ursprünglichen Sinn ein Großrechner, auf den Computer zugreifen, um bestimmte Aktionen auszuführen. Heute wird die Bezeichnung Host auch für Server in einem Rechenzentrum verwendet, der Speicherplatz oder Anwendersoftware für Privatpersonen, Firmen oder Unternehmen zur Verfügung stellt.

Hyperlink

Ein Hyperlink ist ein Querverweis innerhalb eines Dokuments oder auf ein externes Dokument bzw. eine Datei. Wird ein Hyperlink ausgeführt, wird automatisch das darin angegebene Ziel aufgerufen.

On-Premise

Der Begriff On-Premise bezeichnet ein Lizenz- und Nutzungsmodell für serverbasierte Computerprogramme. Die Software wird entweder gemietet oder gekauft und unter eigener Verantwortung im eigenen Rechenzentrum betrieben.

Schadsoftware

Als Schadsoftware werden Computerprogramme bezeichnet, die entwickelt wurden, um auf Computern und Servern unerwünschte und schädliche Funktionen auszuführen. Es gibt unterschiedliche Arten von Schadsoftware, wie z. B. Computer-Viren, Trojaner, Ransomware, Spyware usw.

Service Level Agreements

Ein Service Level Agreement (SLA) bezeichnet eine Vereinbarung zwischen einem Auftraggeber und einem Dienstleister für definierte Dienstleistungen. Das Servicelevel beschreibt das vereinbarte Leistungsspektrum z. B. die Verfügbarkeit und den Umfang der Reaktionszeit des Anbieters zur Wiederherstellung einer bestimmten Dienstleistung.

URL

URL (Uniform Resource Locator) ist ein Verweis auf eine vollständige Pfadangabe, die mit einem handelsüblichen Browser (z. B. Microsoft Edge, Google Chrome, Mozilla Firefox usw.) geöffnet werden kann, zum Beispiel https://www.teamdrive.com/de/.

VPN

Abkürzung für Virtual Private Network (Virtuelles Privates Netzwerk). VPN ist eine Technik, die es ermöglicht, von jedem Ort der Welt sicher auf Ressourcen in einem privaten Netzwerk zuzugreifen. Durch VPN wird eine Internetverbindung in Echtzeit vom Computer zu einem VPN-Server vollständig verschlüsselt.

WebDAV-Server

WebDAV ist ein offener Standard zur Bereitstellung von Daten im Internet. Heutzutage gibt es für jedes Betriebssystem WebDAV-Lösungen, die es ermöglichen, WebDAV-Server (z. B. die MagentaCloud™ der Deutschen Telekom AG) zu implementieren.