T · M · B | Service

IT´s Time for Business

Sicherheitsrisiken der IT-Cloud

www.tmb-service.de/Cloud_Risiko

T·M·B

IT´s Time for Business

Inhalt

T·M·B

IT´s Time for Business

Verletzung und Vertraulichkeit und Integrität der Daten

Sie kennen es auch, es wurde in den letzten zwei, drei Jahren viel Werbung um das Thema Cloud gemacht, wie z.B. ***„Einfach sicher – Das Zuhause für ihre Daten“*** *oder* ***„Die Zukunft der Cloud beginnt jetzt“*** oder was wir als Werbung gefunden haben war ein Logo mit einem ®schaut erstmals vertrauenswürdig aus, richtig?
Verkaufstechnisch eine tolle Überschrift die sich in der Außenwirkung gut lesen lässt. Aber was noch verwirrender ist, dass die bekanntesten Cloud Anbieter wie Dropbox, Google Drive und Microsoft OneDrive noch spannender werben. Man ließt oft ihre Cloud ist nach ***ISO 27001*** zertifiziert, jedoch bedeutet das nicht automatisch, dass die Daten dort sicher sind.

Eine Lokalisierung der Daten ist in einer Public oder Hybrid Cloud für den Dateneigentümer nicht mehr möglich. Daher ist der Schutz der Daten auf der Infrastruktur-/Plattform und Applikationsebene häufig nicht mehr mit üblichen Mitteln zu gewährleisten.

Wir empfehlen die Nutzung von Cloud-Speicherdiensten grundsätzlich nur in Kombination mit zusätzlicher, unabhängiger Verschlüsselungssoftware. Nur so kann verhindert werden, dass Dritte sensible Unternehmensdaten auslesen können. Für den Fall, dass der Cloud-Anbieter angegriffen wird, sind die erbeuteten Daten für die Cyber-Kriminellen nämlich nicht nutzbar. Des Weiteren sind sie auch vor dem Zugriff des Anbieters selbst geschützt. Sogar dann, wenn potentieller Missbrauch durch Behörden und Regierungen droht.

Wir von der TMB Service GmbH können vorab als aller erstes nur eins sagen: ***„Raus aus den US-Clouds“***.

In puncto Datenschutz sind wir als Bundesbürger seit dem 25. Januar 2017 in den USA als Internetnutzer zweiter Klasse gesetzt. Denn US-Präsident Donald Trump hat per Dekret im Januar 2017 erklärt, Nicht-US-Bürger werden vom US-amerikanischen Datenschutzrecht ausgeschlossen oder zumindest unsere Rechte diesbezüglich eingeschränkt. Aber wir nutzen doch Microsoft Produkte und sorgen für den Wachstum einer US-Amerikanischen Firma und werden schlechter behandelt - schade, denken wir uns.

Die weltweit größten Cloud-Speicheranbieter versichern zwar immer wieder, dass Ihre Daten sicher sind, doch hundertprozentige Sicherheit können sie nicht gewährleisten – teilweise aus rechtlichen Gründen, oder da sie es in ihrem eigenen Interesse nicht wollen.

Viele Mitarbeiter der TMB sind zögerlich, wenn es um das Speichern von Daten in der Cloud geht. Der Hauptgrund ist oft die Angst, dass man die Kontrolle über seine EIGENEN DATEN oder die des Kunden aufgeben MUSS.

Die vielen Passwort-Leaks der vergangenen Jahre stärken das Vertrauen in Clouds nicht gerade.

Des Weiteren unterliegen amerikanische Cloud-Anbieter dem amerikanischen Datenschutz, der es leicht möglich macht, diese Daten an US-Behörden zu übergeben.
Große Cloud-Anbieter – in diesem Beispiel Microsoft – machen in Ihren Datenschutzbestimmungen deutlich, dass sie Daten scannen und darauf zugreifen können, hier der Auszug aus der Datenschutzbestimmung von Microsoft:

...Schließlich greifen wir auf persönliche Daten inklusive Ihrer privaten Inhalte (wie die Inhalte … in privaten Ordnern auf OneDrive) zu, legen sie offen und bewahren sie auf, wenn wir in gutem Glauben annehmen, dass dies notwendig ist, um … geltende Gesetze einzuhalten oder auf gerichtliche Verfahren zu antworten.

Seit Einführung der DSGVO biete MS über den personalisierten Account an: „**Verwalten Sie Ihre Datenschutz-Einstellungen.**
Melden Sie sich an, um **Ihre Daten** zu **verwalten**“ wie z.B. Browserdaten, Positionsdaten überprüfen, Suchverlauf löschen von bing, Cortanas Notizbuch bearbeiten.

©OpenClipart-Vectors/pixabay

Wir beraten Sie zum Thema Cloud, mit **SICHERHEIT** ein gutes Gefühl!

T·M·B

IT´s Time for Business

Löschung von Daten

Ist zum Glück in der DSGVO Art. 17 geregelt. Wenn Sie als Betroffenen Person Auskunft über ihre Personen haben möchten, so ist ihrem Wunsch unverzüglich folge zu leisten (Art. 17 Abs. 2 i.V.m. Art. 19 DSGVO). Auch hier besteht das Risiko einer nur unzureichenden Auskunft ihrer Daten oder unvollständigen Löschung z.b. bei einem Socialmedien Anbieter, da alle Plattformen und Datenbanken in der Cloud sind, außerdem ist die Lokalisierung ihrer gesamten Daten nur schwer möglich.

Auch wenn wir mal über den Tellerand hinaus schauen, ist es völlig egal bei welchen Anbieter Sie sind, niemand hat auf seinen Paketpreisen das Thema Löschung nach DoD oder BSI-Standard aufgelistet, obwohl dies unter Funktionen & Preise für verschiedene Cloudpakete immer dargestellt sein MUSS, wenn man sich schon als „seriös“ darstellt.

Es wird ständig mit Tüv-Zertifizierung und DIN-Norm großzügig geworben, die eigenen oder angegebenen Rechenzentren seien nach DIN-Norm 27001 zertifiziert, aber die Löschung nach **DIN-Norm-66398** wird **NICHT** aufgeführt.

Im Mai 2016 ist die neue **DIN Norm-66398** veröffentlicht worden, die den Namen *„Leitlinie zur Entwicklung eines Lösch- Konzepts mit Ableitung von Löschfristen für Personen-bezogene Daten“* trägt und wie folgt definiert ist:

„Die Norm macht Vorschläge zum Aufbau eines Lösch-konzeptes und empfiehlt eine Vorgehensweise, nach der Regeln zum Löschen von personenbezogenen-Daten abgeleitet werden können“.

Die rechtlichen Anforderungen sind im BDSG-neu* unter § 35 Abs. 2 dokumentiert worden. Die nun rechtskräftige DSGVO (Datenschutz-Grundverordnung) benennt in Artikel 5 Abs.1 lit. e dies wie folgt:

„Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.“

Auch nach Vorgabe des **Art.17 DSGVO ->** Recht auf Löschung („Recht auf Vergessenwerden“) beschreibt in Absatz 1 weitere Gründe, wie, personenbezogene Daten wann zu löschen sind:

„Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen...“

Um dies zu gewährleisten, sind Cloud Anbieten um ihre Vertraulichkeit und Integrität gegenüber den Bewohnern die ihre Cloud nutzen, theoretisch auch dazu verpflichtet, die **DIN-Norm-66398** Zertifizierung durchzuführen bzw. öffentlich bekannt darzustellen. Wichtig ist doch, dass man ein Gefühl von Sicherheit bekommt. Wir haben Dialoge mit Kunden geführt, in denen wir folgende Aussagen erhalten haben:
„Ich habe doch nichts zu verheimlichen. Andere nutzen doch auch die Cloud“ oder unser Favorit*:* ***„Es ist doch Microsoft. Die wissen was Sie tun, sonst würden Sie keine Cloud anbieten dürfen“.***

*Seit dem 25. Mai 2018 ist die EU-Datenschutzgrundverordnung (DSGVO) in der gesamten Europäischen Union verbindlich anzuwenden. **Gleichzeitig trat auch ein neues Bundesdatenschutzgesetz in Kraft**, das sogenannte BDSG-neu, das im Bundesgesetzblatt am 5.7.2017 veröffentlicht wurde...
Der Hintergrund ist der, dass die DSGVO zwar unmittelbar geltendes Recht ist und keine Umsetzung in nationales Recht benötigt, wie es bei der alten EU-Datenschutzrichtlinie noch der Fall war – auf den ersten Blick scheint das BDSG-neu also überflüssig zu sein.
Allerdings enthält die DSGVO auch **zahlreiche Öffnungsklauseln**. Das bedeutet, dass an diesen Stellen die Regelungen offengehalten werden, damit sie auf nationaler Ebene konkretisiert werden können. Diese Aufgabe übernimmt das BDSG-neu (Quelle: https://www.datenschutz.org/bdsg-neu/)

Ihr TMB Service Team

Ungenügende Mandantentrennung

Bei nicht ausreichend abgesicherter Mandantentrennung besteht die Gefahr, dass Dritte unautorisierte Daten einsehen oder manipulieren können.

Bezugnehmend auf die weitführende unautorisierten Manipulation von Daten wie z.B. bei WhatsApp, gab es eine negative Rechtssprechung: - wie auch bei zahlreichen anderen Consumer-Apps. Bei WhatsApp wird unberechtigt Zugriff auf Ihre Kontaktdaten genommen, ausgelesen und ohne Berechtigung gespeichert, so wie ein Datenabgleich (mit facebook) auf eigenen Servern in der Clouds durchgeführt.

Damit droht gleich in zweifacher Hinsicht Unheil: So entschied im Mai 2017 das Amtsgericht Bad Hersfeld (Az. F 111/17 EASO), dass allein die Nutzung von WhatsApp gegen das deutsche Datenschutzrecht verstößt. Begründet wurde das Urteil unter anderem damit, dass die App sämtliche Kontaktdaten aus den Smartphones der Nutzer an die WhatsApp Inc. weiterleitet, ohne jedoch die ausdrückliche Zustimmung der Betroffenen einzuholen, dies trifft auch auf die aktuellen Amerikanischen Cloud-Anbieter zu.

Verletzung der Compliance

Da Daten in einer Public Cloud prinzipiell in allen Ländern der Welt in deren spezifischen Rechtsordnungen verarbeitet werden können, ist die Erfüllung aller gesetzlicher Anforderungen eine wesentliche Aufgabe bei der Nutzung von Public Cloud Leistungen.

Auch die Deutsche Bundesregierung will die Sicherheit informationstechnischer Systeme (IT-Systeme) in Deutschland verbessern und hat dazu den Entwurf eines "IT-Sicherheitsgesetzes 2.0" vorgelegt. Es enthält unter anderem Anforderungen an die IT-Sicherheit sogenannter "Kritischer Infrastrukturen", also der Einrichtungen, die für das Funktionieren des Gemeinwesens von zentraler Bedeutung sind.

Die DSGVO zeigt erste Zähne: 50-Millionen-Strafe gegen Google verhängt!
Die französische Datenschutzbehörde **Commission Nationale de l'Informatique et des Libertés** (CNIL) hat gegen Google eine Rekordstrafe in Höhe von 50 Millionen Euro verhängt. Die Behörde kreidet Google zwei Verstöße gegen die Datenschutzgrundverordnung (DSGVO) an. **Erstens** missachte der Konzern die Pflicht, seine NutzerInnen transparent über die Datennutzung zu informieren. Zweitens könne der Konzern keine wirksame Einwilligung für die Verarbeitung der Daten für Werbezwecke vorweisen.

In der Pressemitteilung der CNIL heißt es: *„Wesentliche Informationen, wie die Zwecke der Datenverarbeitung, die Aufbewahrungsfristen oder die Kategorien von personenbezogenen Daten, die für die Personalisierung der Anzeigen verwendet werden, sind zu sehr auf mehrere Dokumente verteilt, mit Buttons und Links, auf die geklickt werden muss, um auf zusätzliche Informationen zuzugreifen." Zudem sei der Zweck der Datenerhebung zu allgemein und vage beschrieben.*

Weiter heißt es in der Pressemitteilung zu **Verstoß zwei:**
[...] das Google keine wirksame Einwilligung der Nutzer:innen für die Nutzung ihrer Daten zu Werbezwecken vorweisen können. Aufgrund der ungenügenden Informationen könnten Menschen nicht einschätzen, welche anderen Google-Dienste und Webseiten (Youtube, Maps, Drive) in die Auswertung ihrer persönlichen Daten involviert sind.

T·M·B

IT´s Time for Business

Verletzung von Datenschutzrechten.

Es ist nicht von vornherein klar, in welchen Ländern, Rechenzentren, auf welchen Servern und mit welcher Software die Daten gespeichert und verarbeitet werden. Werden diese auf Verlangen auch gelöscht? Um diese und mehr Themen zu vereinheitlichen wurde die EU-DSGVO in Kraft gesetzt.

Als bestes Beispiel führen wir den, als „Normal“ im Alltag angekommenen, Social Media Anbieter Facebook auf:

Nach § 13 Abs. 1 TMG sind Online-Dienstanbieter dazu **verpflichtet**, Nutzer zu Beginn des Nutzungsvorgangs **über** Art, **Umfang** und **Zweck** der **Erhebung, Verwendung** und **Verarbeitung** personenbezogener **Daten** zu **unterrichten**. **Facebook** selbst **schweigt** sich über **Inhalt** und **Umfang** der Datenerhebung und der **Verarbeitung** aus. Was das Unternehmen mit den gewonnenen Konsumprofil seiner Mitglieder macht ist unklar. Aber was man weiß ist, Sie verdienen Geld ohne das die Nutzer was davon mitbekommen und zwar Medienberichten zufolge bis zu 3 EUR-Cent pro Bild, Status, Kommentar, Gefällt mir oder anderweitige Aktivität auf der Plattformen.

Der Nutzer wird hierrüber, entgegen § 13 Abs. 1 TMG, nicht informiert.
Die Betreiber von Websites mit „Gefällt mir“ Plug-ins **wissen** selbst **nicht**, was Facebook **mit den** gewonnenen **Daten anstellt**. Was aber bekannt ist, dass Betreiber die auf ihrer Website dieses „Gefällt mir“ Plugin zur Verfügung stellen oftmals NICHT wissen, dass ihre Kundendatenbank Inhalte kopiert und die Bestellungen „gescannt“ und die Käufer auf Grund ihres angelegten Käuferprofils in Facebook integriert werden und wenn man sich dann bei Facebook anmeldet, erhält man auf einmal „Werbung“ wie z.B. „könnte dir gefallen“ Angebote, die direkt personalisiert sind. Die Betreiber befinden sich in dem Dilemma, dass sie die Besucher ihrer Website nicht ordnungsgemäß unterrichten können, selbst wenn sie es wollten.

Die Rechtswidrigkeit ihres Handelns steht gleichwohl außer Frage, da jeder Seitenbetreiber als „Verantwortliche Stelle“ im Sinne des Bundesdatenschutzgesetzes und der DSGVO angesehen wird, sobald er personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere (z.b. facebook) vornehmen lässt.

Aufgeführt die Vor- und Nachteile einer Cloud aus Anwendersicht:

Vorteile

- Flexible und bedarfsorientierte Verfügbarkeit der IT
- Kein Wartungsaufwand für und Investitionen in Soft- und Hardware
- Leistungsbezogene Vergütung und Kostenkontrolle
- Höhere Leistung und bessere Performance (Spezialisierung und Skalierbarkeit beim Dritten „Systemhausgeschäft“).
- Zugriff auf vorkonfigurierte Umgebung
- Nutzt Software ohne eigenständige Installation
- Zertifizierung nach DIN-Norm-27001

Nachteile

- Daten (Schutz) Sicherheit
- Geheimhaltung
- Verfügbarkeit der Cloud
- Remigration oder Transition auf andere Anbieter
- keine Individualisierbarkeit der „Cloud“
- Kein (Unmittelbarer) Einfluss auf Qualität der gebuchten Services
- Abhängigkeit von Dritte bei Leistungserbringung
- Wirtschaftsspionage
- Fehlende oder mangelnde Maßnahmen zur Umsetzung der Compliance
- Oft keine Zertifizierung nach DIN-Norm-66398

Insolvenz des Providers

Die Insolvenz eines Providers bedeutet meist nicht die Insolvenz aller Rechenzentren, die der Provider verwendet hat. Rechenzentren werden zudem bei Insolvenz mit großer Wahrscheinlichkeit an andere Provider verkauft.

Problematik der Subunternehmer

Ein weiteres Problem stellt die Auftragsweitergabe an Subunternehmer dar. Der Provider wird häufig Subunternehmer für gewisse Leistungen verpflichten. In einer Public Cloud bleibt auch diese Komplexität dem Benutzer häufig verborgen (und soll ja nach der Philosophie des Cloud Computing verborgen bleiben).

Was auch nicht bekannt ist:
Ist die Serverfarm die eigene des Anbieters oder wirbt dieser nach außen mit einer eigenen Farm, aber unterwirft sich Kontrolle und Anforderungen eines unabhängigen Dritten?

Daher ist es immer sinnvoll, zu prüfen:
Ist der Cloud Anbieter Zertifiziert nach Art. 42 DSGVO: Mitgliedstaaten, Aufsichtbehörden, Ausschuss EU-Kommission sollen Einführung datenschutzspezifischer Zertifizierungsverfahren, Datenschutzsiegel und Prüfzeichen fördern.
Rahmenbedingungen für Zertifizierungsverfahren: Art. 42 und 43 DSGVO

- **Was** wird zertifiziert? Ein Datenverarbeitungsvorgang und KEIN Produkt, KEINE Dienstleistung
- **Ziel:** Nachweis, dass entsprechende Verarbeitung im Einklang mit der DSGVO
- **Wer** Zertifiziert? Zertifizierungsstelle oder zuständige Aufsichtsbehörde nach festgelegten Zertifizierungskriterien: Art. 42 Abs.5, Art 57 Abs. 1 lit. n), Art. 70 Abs 1 lit. n), Art 43 Abs. 9 DSGVO

Beschlagnahmung von Hardware

Eine Beschlagnahme von Hardware kann in allen Ländern erfolgen, in denen der Provider Computing-Ressourcen nutzt. Meist werden sich Daten des Auftraggebers auf beschlagnahmten Servern befinden und denkbar ist auch, dass Provider vorab einen Handel mit ihren Ressourcen untereinander aufbauen und damit eine "Ressourcenbörse" realisieren. Auf diesen Börsen werden Ressourcen zu einem bestimmten Preis angeboten – JE mehr DATEN je MEHR GELD und bei einer Insolvenz möchte jeder Inhaber noch ein wenig Umsatz generieren.

Was dann im Anschluss passieren kann ist, dass die Gefahr von Erpressungsversuchen durch die Käufer ihrer Daten vom Insolventen Anbieter steigt, da der Käufer Ihre Daten für viel Geld erworben hat, möchte er seine Investition um jeden Preis vermehren und sicherlich nicht nur um das dreifache – Gehandelt werden diese Daten überwiegend im „Darknet“.

Mit SICHERHEIT eine gute Entscheidung –
Der IT-Audit für mehr Konformität in ihrem Unternehmen!

Haben Sie Fragen? – Kontaktieren Sie uns!

T·M·B | Service

aus Lünen an der Lippe

TMB Service GmbH
Am Brambusch 24
44536 Lünen
Tel.:0231/98 60 570

info@tmb-service.de
www.tmb-servie.de

audIT **IT-Consulting** **IT-Security** **IMAC** **IT-Support** **IT-RollOut** **DSGVO**

Hier finden Sie uns: