SCHÜLERMAPPE

SELBSTLERNEINHEIT

Berufsschüler BOTTOM-UP! für IT-Sicherheit

LERNEINHEIT 5: CLOUD-DIENSTE UND DATENSCHUTZ IM UNTERNEHMEN

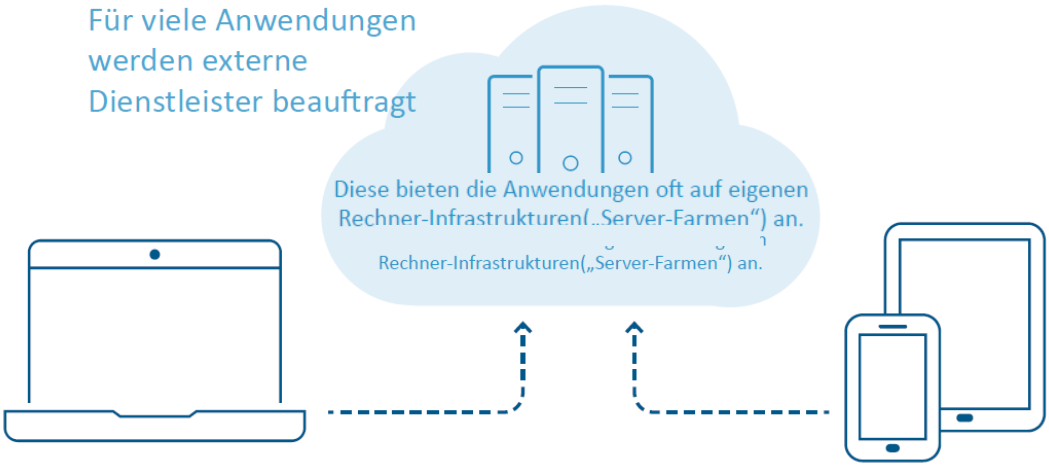
Onlinedienste und Cloud Computing werden in nahezu jedem Unternehmen eingesetzt. Sie bieten neue Möglichkeiten und vielfältige Vorteile für Unternehmen, gleichzeitig bringen sie jedoch **spezifische Risiken und Anforderungen** mit sich. Vor- und Nachteile bei der Cloud-Nutzung sowie **datenschutzrechtliche** Fragen sind im Vorfeld zu klären.

DIE THEMEN:

*Obwohl aus Gründen der Lesbarkeit im Text die männliche Form gewählt wurde, beziehen sich die Angaben auf Angehörige aller Geschlechter.

1. ÜBERALL ERREICHBAR: ONLINE-DIENSTE IN DER CLOUD

Unternehmen benötigen unterschiedliche IT-Anwendungen: E-Mail-Postfächer, eine Webseite, Buchhaltung sowie die Erstellung und Verwaltung verschiedenster Dokumente. Daneben existiert eine Vielzahl von branchenspezifischen Applikationen, beispielsweise zur Steuerung von Maschinen, Erhebung und Auswertung von Daten oder Überwachung einer Fahrzeugflotte.



Der Zugriff auf die Anwendungen erfolgt über das Internet

Cloud und Server Farmen.

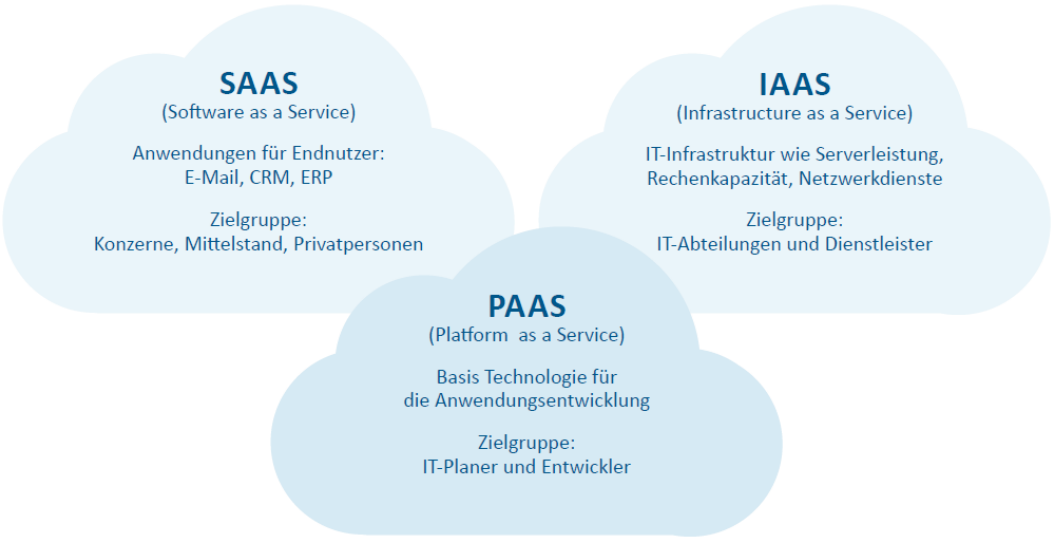
Diese bieten die jeweiligen Anwendungen dann auf ihrer eigenen Rechner-Infrastruktur („Server Farmen“) an. **Der Zugriff auf die Anwendungen durch die Kunden erfolgt über das Internet**. Man spricht dabei oft vom „**Cloud Computing**“, da Daten nicht zentral, sondern auf eine Vielzahl verschiedener Rechner gespeichert werden, die zusammen eine sinnbildliche Wolke ergeben.

LINK

Wer es genau wissen will – die **Grundbegriffe des Cloud Computing** sind in zwei Standards definiert:

> **The NIST Definition of Cloud Computing** aus dem Jahr 2011 http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

> ISO/IEC 17788:2014 – **Information technology — Cloud computing — Overview and vocabulary**. Normalerweise kostenpflichtig, für Bildungszwecke aber kostenfrei erhältlich. http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html



Unterschieden werden hierbei **drei Typen von Dienstleistungen,** je nachdem, wo sie in der Cloud-Computing-Architektur angesiedelt sind:

> **Software as a Service (SaaS):** Wird Software nicht mehr als abgeschlossenes Produkt an Endkunden verkauft, sondern über die Cloud zu Verfügung gestellt, spricht man von Software as a Service. Konkrete Beispiele hierfür sind E-Mail-Anbieter, onlinebasierte Dokumenten-, Tabellen- und Präsentationssoftware oder Anwendungen für Unternehmen wie ein cloudbasiertes Customer Relationship Management-System (CRM). Zielgruppe von SaaS sind Endanwender: Konzerne, Unternehmen, Privatpersonen.

> **Platform as a Service (PaaS)**: Richtet sich hingegen vorwiegend an IT-Planer und -Entwickler. Über verschiedene von Herstellern bereitgestellte Schnittstellen und Plattformen können diese eigene Programme und Anwendungen entwickeln. Dementsprechend werden über PaaS in der Regel Programmierumgebungen und Anwendungsentwicklungssysteme angeboten. Dabei haben Entwickler keinen direkten Zugriff auf die Infrastruktur, über die das jeweilige Angebot bereitgestellt wird.

> **Infrastructure as a Service (IaaS):** Hier wird von Anbietern Infrastruktur zu Verfügung gestellt, darunter vor allem Serverleistung, Rechenkapazität, Speicher oder Netzwerkdienste. Die Hardware wird dabei vom Anbieter der Server Farm betreut während der Kunde diese über das Internet steuern und nutzen kann. Zielgruppe von IaaS sind ganze IT-Abteilungen oder IT-Dienstleister.

E-Mail als SaaS

Viele Unternehmen greifen auf SaaS bei E-Mail in Kombination mit Spam- und Virenfilter zurück.

Die E-Mail-Infrastruktur einer Firma ist oft als **Software as a Service (SaaS)** implementiert. Es gibt zahlreiche Anbieter, die E-Mail-Adressen anbieten. Für Privatnutzer sind das zum Beispiel Hotmail, Yahoo, Gmail und viele mehr. Ähnliche Dienstleistungsanbieter existieren auch für Unternehmen, die dann den Versand und Empfang unter der Webadresse der Firma organisieren. Die Anbieter kümmern sich in diesem Fall um alle Bestandteile der Architektur: Sie betreiben eine Server Farm, auf deren Rechner die E-Mail-Software läuft und über Internet den Nutzern zu Verfügung gestellt wird. Im Rahmen solcher Lösungen werden häufig auch Spam- und Virenfilter als SaaS integriert.

Webseite als SaaS, PaaS oder IaaS?

Die Onlineauftritte von Unternehmen können unterschiedlich realisiert werden. Werden von Anbietern bereitgestellte, schlüsselfertige **Content Management Systeme (CMS)** genutzt, die auf der Infrastruktur des Anbieters bereitgestellt werden, handelt es sich um einen klassischen SaaS-Ansatz. Die großen **Vorteile**: Das Unternehmen muss sich **nicht um die Wartung und Pflege** der Infrastruktur kümmern, gleichzeitig kann es dank des CMS die Inhalte selbst verwalten und aktuell halten.

IaaS bietet die größtmögliche Flexibilität, während SaaS am wenigsten eigene Wartung vom Unternehmen verlangt.

Am anderen Ende des Spektrums gibt es IaaS-Lösungen, bei denen Unternehmen nur die Infrastruktur für die eigene Webseite von einem Anbieter beziehen. Es werden also Server angemietet, auf denen die Webseite dann „gehostet“ wird, die Dienstleistung wird dementsprechend **Serverhosting** genannt. Diese Lösungen kommen insbesondere dann in Frage, wenn das Unternehmen den eigenen Internetauftritt komplett selbstständig mit maximaler Gestaltungsfreiheit entwickeln will oder besondere Anforderungen vorliegen, die vorgefertigte SaaS- oder PaaS-Lösungen nicht erfüllen können.

Virtualisierung von Servern

Wird ein Serverhosting-Angebot genutzt, steht dabei nicht immer ein tatsächlicher, einzelner physischer Server dahinter. Je nach Anwendungsprofil ist dies auch nicht nötig – bei weniger rechenintensiven Anwendungen hätte ein einzelner Server erhebliche ungenutzte Überkapazitäten. Vielmehr laufen stattdessen in den großen **Rechenzentren** der Anbieter Programme, die solche **Server simulieren**. Dies wird als **virtuelle Maschine oder virtueller Server** bezeichnet. Diese Form der Virtualisierung ermöglicht es, die Rechnerkapazitäten kurzfristig und flexibel an die Bedürfnisse des Marktes und der Kunden anzupassen.

Braucht der Kunde hingegen einen schnellen, leistungsstarken Server, auf dem rechenintensive Anwendungen laufen können, werden ihm eine oder sogar mehrere physisch eigenständige Maschinen zur Verfügung gestellt. Hier spricht man dann von **dedicated Servern**.

Selten: PaaS (Platform as a Service)

Der Einsatz von PaaS-Anwendungen ist für die meisten kleineren Unternehmen eher die Ausnahme. Solche Angebote richten sich zumeist an spezialisierte Unternehmensanforderungen. PaaS-Anbieter ermöglichen es ihren Kunden, bestimmte spezialisierte Plattformen als Grundlage für eigene Anwendungen laufen zu lassen und ersparen ihnen die Arbeit, sich um die Konfiguration des darunterliegenden Betriebssystems zu kümmern.

Onlinespeicher und Dokumentenverwaltung

Typische Cloud-Dienste im Internet für KMU und Verbraucher.

In den letzten Jahren haben sich vor allem Dienste durchgesetzt, die das **Verwalten und den Austausch von Dokumenten** ermöglichen. Neben dem Zugriff auf die Dokumente von verschiedenen Orten bieten viele dieser Anbieter eine **Versionsverwaltung**. So können mehrere Mitarbeiter gleichzeitig am selben Dokument arbeiten. Bei der Auswahl des Anbieters sollten einige Aspekte beachtet werden:

> Werden die gespeicherten Dateien und Dokumente vor dem Hochladen in die Cloud vom Dienstanbieter verschlüsselt? Ansonsten könnten der Anbieter der Cloud oder unbefugte Dritte, die sich einen Zugang verschaffen, alle Daten einsehen. Alternativ kann man die Daten auf dem lokalen Rechner oder Gerät selber verschlüsseln, als verschlüsseltes Archiv beispielsweise, bevor man sie in die Cloud hoch lädt.

Sichere Passwörter: siehe Lerneinheit 1!

> Ist der Zugang zum Dienst bzw. den Dokumenten mit einem Passwort versehen? Natürlich sollte auch der Zugang zum Cloud-Dienst mit einem hinreichend sicheren Passwort vor Angriffen geschützt sein.

Wo genau werden die Daten gehostet? Wo befinden sich die Server des Dienstes? Diese Frage kann eine Rolle spielen, welche Art von Daten man bei welchem Dienst hosten lässt, um die Sicherheit vor dem Zugriff Dritter zu erhöhen, vor allem, wenn man die Daten und Dateien aus Gründen der Nutzerfreundlichkeit nicht verschlüsseln möchte.

Kalendertools

Großer Beliebtheit erfreuen sich diverse Tools zur Verwaltung von Kalendern. **Eine Vielzahl von Dienstleistern** bietet jeweils eigene Cloud-Services an, die die Synchronisierung eigener Kalender über unterschiedliche Geräte ermöglichen. Unternehmen sollten sich vor dem Einsatz dieser Tools überlegen, welche Sicherheitsanforderungen aus dem jeweiligen Einsatzszenario entstehen, und welcher Dienst und Dienstleiser daraufhin ausgewählt wird. Die Sicherheitsanforderungen sollten auch bei der Verwaltung von Terminen nicht aus Gründen der Bequemlichkeit vernachlässigt werden. Eine **Verschlüsselung der Termine** auf dem gehosteten Webservice und eine **verschlüsselte Übertragung** der Daten an den Webservice sind für Unternehmen stets zu empfehlen.

Der eigene Cloud-Server

Ein Unternehmens-eigener Cloud-Server verlangt eine kompetente IT-Abteilung.

Unternehmen gehen zunehmend dazu über, ihre **eigene Cloud-Infrastruktur** zu verwalten. Die Gründe hierfür sind vielfältig. Neben den im folgenden Kapitel genannten Nachteilen des Cloud Computing, spielt die **Angst vor Industriespionage** immer wieder eine Rolle. Eine eigene Unternehmens-Cloud ist aber nahezu immer auch auf eine **kompetente IT-Abteilung angewiesen**, die diese Systeme wartet. Für kleinere Unternehmen stellt das oft eine erhebliche Hürde dar. Aber auch für diese Unternehmen entwickeln sich langsam erste Angebote mit technisch einfachen Lösungen, die wartungsarm zu betreiben sind. Gleichzeitig **wächst aber auch die Nachfrage nach Dienstleistern**, die sich um die Wartung und Absicherung von unternehmenseigener Infrastruktur kümmern.

2. VOR- UND NACHTEILE DES CLOUD COMPUTING

Man sollte jeweils im Einzelfall sorgfältig abwägen, ob die Vorteile eines Onlinedienstes die Nachteile überwiegen.

BEISPIEL

Die kleine IT-Firma „Ansbucher Computermanager GmbH“, die regelmäßig Computer bei ihren Kunden wartet und austauscht, ist vor Jahren begeistert in die Cloud eingestiegen. Alle ihre Dokumente werden nur in der Cloud verwaltet. Nach drei Jahren jedoch geht der Anbieter plötzlich insolvent. Nun muss schnell Ersatz gefunden und die Datenbestände übertragen werden. Eine Migrationsstrategie hat bislang weder auf Seiten der IT-Firma noch auf der des Cloud-Anbieters existiert, und so stehen den Administratoren einige Nachtschichten bevor…

Vorteile des Cloud Computing

Cloud-Computing kann eine Vielzahl von **Vorteilen** bieten, zum Beispiel:

> Die Auftraggeber können flexibler bestimmen, wie viel Rechenkapazität sie benötigen, ohne dass sie jedes Mal neue Hardware anschaffen müssen.

> Die **Zuverlässigkeit** der IT-Infrastruktur kann verbessert werden, weil jederzeit Ersatzhardware zur Verfügung steht.

> Die Qualität und **Wartung** der Systeme kann fortlaufend durch die Spezialisten des Anbieters überwacht werden, ohne dass sich der Auftraggeber darum kümmern muss.

> Weil Cloud-Dienste über das Internet erreichbar sind, können Mitarbeiter von überall her darauf zugreifen, etwa auf **Dienstreisen** oder aus dem **Homeoffice**.

Vorteile und Nachteile des Cloud Computing müssen abgewogen werden.

Nachteile des Cloud Computing

Für ein Unternehmen kann Cloud Computing – je nach Einsatzgebiet – auch Nachteile mit sich bringen, die man sich bewusst machen muss, damit man entsprechende Schutz- und Sicherungsmaßnahmen (**siehe Kapitel 3**) ergreifen kann.

> Die Rechner-Infrastruktur des Unternehmens steht nicht vollständig unter der **Kontrolle** des Unternehmens. Interne Dokumente und Kundendaten können bei unzureichenden Sicherheitsmaßnahmen potenziell in falsche Hände geraten.

> Systeme, die über das Internet zugänglich sind, sind anfälliger gegen **Angriffe von außen**. Das bedeutet, dass Unternehmen dafür sorgen müssen, dass ihre internen Dokumente und Kundendaten etwa durch Verschlüsselung gesichert werden.

> Unternehmen begeben sich in eine **Abhängigkeit** vom Cloud-Anbieter (Lock-In Effekt). Geht dieser in Konkurs, kann dies die Unternehmen, die dort Produkte nutzen, unter Umständen ebenfalls gefährden.

> Die **Verantwortung** für die Verarbeitung personenbezogener Daten bleibt auch bei der Beauftragung von Cloud-Dienstleistern rechtlich beim (Auftrag gebenden) Unternehmen. Daher ist besondere Sorgfalt geboten.

LINKTIPP

Das Bundesministerium für Wirtschaft und Energie bietet mit **Trusted-Cloud** ein Informationsportal mit vertrauenswürdigen Cloud-Anbietern: https://www.trusted-cloud.de

VORTEILE

> Flexibilität in der Ausrichtung am Bedarf

> Zuverlässigkeit der IT-Infrastruktur

> Sicherstellung von Qualität und Wartung

> Verfügbarkeit außerhalb des Büros

NACHTEILE

> „Verlust“ der Kontrolle über Infrastruktur

> Potenzieller Angriffspunkt durch Onlineverfügbarkeit

> Abhängigkeit vom Cloud-Anbieter

3. SICHERUNGSMAßNAHMEN

Ist man sich der besonderen Herausforderungen hinsichtlich der Risiken bei Cloud-Computing bewusst, kann man **effektive Schutzmaßnahmen** ergreifen, um diese Risiken zu minimieren oder sogar vollständig zu eliminieren. Dieser Abschnitt wird verschiedene Schutzmaßnahmen, Anforderungen und Abwägungen thematisieren, damit einer sicheren Nutzung von Cloud-Diensten nichts im Wege steht.

Zunächst sollte der Einsatz von Onlinediensten nie **ohne eine explizite Entscheidung des Unternehmens** erfolgen. Wer als Mitarbeiter Kundendaten einfach an einen Cloud-Speicher überträgt, riskiert Abmahnung und Kündigung durch den Arbeitgeber!

WICHTIG

Niemals ohne Rücksprache im Unternehmen Daten auf bisher noch nicht verwendete Online-Dienste kopieren. Die Nutzung muss stets abgestimmt sein.

Bei der Beauftragung eines Anbieters muss überprüft werden, ob dieser für die beabsichtigte Nutzung verlässlich genug ist. Kriterien, die hierbei berücksichtigt werden sollten, sind:

Wie hoch ist die vom Anbieter versprochene Ausfallsicherheit?

Eine Ausfallsicherheit von 99% ist übertragen auf das Jahr 3,5 Tage.

Garantiert der Anbieter eine **hinreichend hohe Ausfallsicherheit**? Eine Ausfallsicherheit von 99 Prozent mag auf dem ersten Blick für viele Fälle ausreichend erscheinen. Man sollte aber bedenken, dass damit ein Ausfall des Systems an 3,5 Tagen im Jahr noch im versprochenen Rahmen bleibt. Für viele Anwendungsfälle ist das nicht akzeptabel. Zum Glück bieten viele Anbieter eine deutlich höhere Ausfallsicherheit. So bieten Server Farmen beispielsweise zahlreiche **Redundanzen und Rückfallmöglichkeiten**, sollte doch mal ein Server ausfallen. Eine hundertprozentige Sicherheit gibt es jedoch nie – allerdings trifft das nicht nur auf Cloud-Dienste zu.

Welche Migrationsmöglichkeiten bietet der Anbieter?

Insbesondere bei spezialisierten Anwendungen ist es wichtig, dass Unternehmen bei der Auswahl eines Anbieters prüfen, inwiefern **die Daten zu einem späteren Zeitpunkt zu einem anderen Anbieter migriert werden können**. Ist eine solche Möglichkeit nicht gegeben, muss sich das Unternehmen im Klaren darüber sein, dass eine **gewisse Abhängigkeit vom Anbieter** droht. Fällt der Anbieter beispielsweise temporär oder dauerhaft aus, kann das für ein Unternehmen ein ernstes Problem sein, wenn ein Umzug zu einer Alternative nicht möglich ist. Es lohnt sich somit vorab ein ausführlicher Vergleich der Anbieter, der von ihnen genutzten Standards sowie der Möglichkeiten, Daten zu ex- und importieren.

Welche Verschlüsselungsmöglichkeiten bietet der Anbieter?

Sichere Übertragung vs. Sichere Verwahrung der Daten.

Bei jeder Übertragung von Daten ist darauf zu achten, dass die Daten an allen Stellen durch **geeignete Maßnahmen vor unbefugtem Zugriff** gesichert sind. Grundsätzlich kann man zwischen der **sicheren Übertragung und sicheren Verwahrung** der Daten unterscheiden.

Die **Übertragung** wird in der Regel dadurch gesichert, dass die Daten **verschlüsselt** übertragen werden. Bei Anwendungen, die über Webbrowser genutzt werden, erfolgt dies beispielsweise durch eine https-Verbindung.

Bei der sicheren Verwahrung der Daten in der Cloud muss zwischen zwei Szenarien unterschieden werden, die aber auch kombiniert werden können:

Verschlüsselung durch den Anbieter oder Verschlüsselung durch den Anwender

> Viele **Anbieter** bieten von sich aus die Möglichkeit, die vom Kunden in die Cloud transferierten Daten **dort verschlüsselt zu speichern**. In solchen Fällen kann in der Regel selbst der Anbieter die Daten nicht auslesen – nur der Kunde kann sie dank eines Passworts einsehen.

> Alternativ kann der Kunde die Daten **vor dem Transfer in die Cloud lokal selbst verschlüsseln**. Dies empfiehlt sich vor allem bei Anbietern, die keine oder eine nur unzureichende Verschlüsselung anbieten. Dies ist bei vielen kostenfreien Cloud-Diensten der Fall. Zur lokalen Verschlüsselung gibt es verschiedene Programme, von denen einige nahtlos in Cloud-Dienste integriert werden können, sodass der resultierende Aufwand minimiert wird.

Was für Berechtigungskonzepte unterstützt der Anbieter?

Ein **Berechtigungskonzept** regelt die Zutritts-, Zugangs- und Zugriffskontrolle auf Programme, Daten und Systeme. Da bei Cloud-Diensten die Daten nicht auf den unternehmenseigenen Rechnern gespeichert werden, sondern auf entfernten Server Farmen des Anbieters, ist ein Unternehmen bei der Umsetzung eines Berechtigungskonzepts auf die Möglichkeiten des Anbieters angewiesen. Bei der Auswahl eines Anbieters sollte eingehend überprüft werden, ob er alle Anforderungen des Unternehmens erfüllt.

BERECHTIGUNGSKONZEPTE

Ein Berechtigungskonzept ist aber auch oft für das Unternehmen, das den Dienstleister beauftragt, sinnvoll. In den meisten Fällen soll ja nicht jeder Mitarbeiter auf Daten und Ressourcen der Firma Zugriff haben. Hierfür werden erst einmal verschiedene Rollen definiert. Anschließend erfolgt die Zuordnung von ein oder mehreren Rollen zu jedem Mitarbeitenden. Zum Schluss erhalten bestimmte Rollen die Zugriffsberechtigung für bestimmte Datenbestände. Sie werden ggf. auch mit entsprechenden Maßnahmen ausgestattet, die einen unbefugten Zugriff unterbinden. So haben dann etwa nur Mitarbeiter mit der Rolle „Personalabteilung“ Zugriff auf die komplette (digitale) Personalakte.

Wie können Daten gesichert, aber auch sicher gelöscht werden?

Bei der Auswahl eines Anbieters ist es wichtig, sich vorab damit zu beschäftigen, inwiefern und wie das System, die Anwendung oder die Plattform eine Verwaltung der Daten durch den Kunden ermöglicht:

> Wie erfolgt beispielsweise die **Datensicherung** (Backups)?

> In welchen Zeitabständen?

> Wie lange werden die Sicherheitskopien aufbewahrt?

> Aber auch umgekehrt: Kann eine Datenlöschung sichergestellt werden, wenn die Daten nicht mehr benötigt werden?

Zu klärende Fragen:

1. Ist die Ausfallsicherheit garantiert?
2. Gibt es eine Migrationsstrategie?
3. Sind die Daten durch Verschlüsselung geschützt?
4. Liegt ein Sicherheitskonzept vor?
5. Wie sieht das Berechtigungskonzept aus?

4. DATENSCHUTZASPEKTE

Rechtliche Verantwortung für Verarbeitung personenbezogener Daten liegt weiterhin beim Unternehmen.

Sofern – wie in den allermeisten Fällen – personenbezogene Daten verarbeitet werden sollen, muss das **Datenschutzrecht** beachtet werden. So wie die Mitarbeiter eines Unternehmens auf die Einhaltung des Datengeheimnisses vertraglich verpflichtet werden müssen, gibt es natürlich auch Pflichten für den Cloud-Dienstleister. Die **rechtliche Verantwortung verbleibt aber nahezu immer beim Auftrag gebenden Unternehmen**. Dieses haftet also auch für die Fehler und Datenschutzverstöße des Cloud-Dienstleisters. Daher muss es besonders sorgfältig auf die Einhaltung des Datenschutzes beim Dienstleister achten.

LINKTIPP

Hier geht es zur BITKOM-Studie „Vertrauen und Sicherheit im Netz“:

http://t1p.de/ej6m

Auftragsdatenvereinbarung zentraler Vertragsbestandteil mit Cloud-Anbietern.

Verpflichtend ist dabei, dass der Auftragnehmer eine sogenannte **Auftragsdatenvereinbarung** unterschreibt. Diese dient dem Zweck, einen sorgfältigen Umgang des Auftragnehmers mit den Daten abzusichern. Gemäß **Bundesdatenschutzgesetz** (BDSG) muss eine Auftragsdatenverarbeitung zwischen Auftraggeber und Auftragnehmer unterzeichnet werden, sobald personenbezogene Daten durch den Auftragnehmer verarbeitet werden. Dies betrifft beispielsweise klassische Aufträge zur Lohn- und Gehaltsabrechnung, oder zur Finanzbuchhaltung. Aber genauso sind durch Outsourcen in die Cloud auch Telekommunikations- und E-Mail-Dienstleistungen, Archivierung und Backups, und sonstige Datendienste von der Vorschrift betroffen.

In der Auftragsdatenverarbeitung müssen ebenso die zu treffenden **technischen und organisatorischen Maßnahmen**, die vom Auftragnehmer zum Schutz der zu verarbeitenden personenbezogenen Daten getroffen werden, festgelegt werden. Dies betrifft insbesondere die Maßnahmen zur **Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags-, Verfügbarkeits- und Trennungskontrolle** (siehe auch Anlage zu § 9 BDSG). Mustertexte für eine Auftragsdatenvereinbarung können bei den **Datenschutzbehörden** heruntergeladen werden.

Die Einhaltung dieser Vereinbarung muss durch den Auftraggeber zudem durch **Stichproben** überprüft werden – etwa indem er sich selber vor Ort von den Kontrollmaßnahmen ein eigenes Bild macht. Dies ist besonders für kleinere Unternehmen oftmals nicht praktikabel. Daher sollten KMU bei der Auswahl der Cloud-Anbieter sehr aufmerksam sein.

LINKTIPP

Formulierungshilfe für datenschutzrechtliche Vertragsregelungen vom Bayerischen Landesamt für Datenschutzaufsicht:

https://www.lda.bayern.de/media/info_adv.pdf

Speicherung von Daten außerhalb der EU: gesonderte Anforderungen verlangt.

Rechtlich schwierig ist allerdings die Fallkonstellation, wenn der Cloud-Dienstleister gar **keinen Firmensitz in Europa** hat. Dies ist dann tatsächlich nur in seltenen Ausnahmefällen rechtlich zulässig. Verarbeitet oder speichert ein Cloud-Dienstleister **Daten außerhalb der EU**, gelten besondere Anforderungen an den Vertrag zwischen Auftraggeber (auch Datenexporteur genannt) und Auftragnehmer (Datenimporteur). Diese stellen sicher, dass trotz abweichender Datenschutzrichtlinien im Zielland das „angemessene Datenschutzniveau" eingehalten wird. Grundsätzlich gilt auch hier, dass das **Unternehmen**, das eine Cloud-Anwendung nutzt, **dafür verantwortlich und haftbar ist,** dass den Datenschutzrichtlinien entsprochen wird.

Die EU hat für solche Szenarien **Standardvertragsklauseln** erlassen, die von den Anbietern in Verträgen seit 2010 unverändert übernommen werden mussten. Diese Standardvertragsklauseln decken jedoch nicht alle Anwendungsmöglichkeiten ab, weshalb teilweise zusätzliche vertragliche Vereinbarungen mit den Anbietern von Cloud-Diensten erforderlich sind

HINTERGRUND: SAFE HARBOUR UND PRIVACY SHIELD

Für Anbieter aus den USA gab es bis Oktober 2015 das sogenannte **Safe Harbor-Abkommen**, im Rahmen dessen sich Anbieter zertifizieren lassen konnten, um zu bescheinigen, dass sie personenbezogene Daten **gemäß der europäischen Datenschutzrichtlinie** verarbeiten. Das Abkommen wurde jedoch vom **Europäischen Gerichtshof** für **ungültig** erklärt, weil es die Daten nicht ausreichend vor dem Zugriff durch US-amerikanische Sicherheitsbehörden geschützt hat. Das Nachfolge-Abkommen **Privacy-Shield** trat Mitte 2016 in Kraft. Eine Liste mit den amerikanischen Firmen, die unter dem Abkommen agieren, ist einsehbar unter:

https://www.privacyshield.gov/list.

LINKTIPP

Wer die Cloud für personenbezogene Daten nutzen will, muss sich oft intensiv mit den jeweiligen Risiken auseinandersetzen. Einen Überblick bietet der „**Leitfaden Datenschutz und Cloud Computing**" des Kompetenzzentrums „Trusted Cloud" unter:

http://t1p.de/c3li (verkürzter Link)

LÜCKENTEXT L5 „CLOUD-DIENSTE IM UNTERNEHMEN NUTZEN“

ARBEITSBOGEN

Den folgenden Lückentext können Sie alternativ auch in Form eines Online-Spiels direkt auf ihrem Computer ausfüllen.

Der Online-Lückentext ist verfügbar auf der Bottom-Up-Webseite unter: https://www.dsin-berufsschulen.de/unsere-online-lueckentexte.

Arbeitsauftrag

Füllen Sie auf Basis der Inhalte im vorangegangenen theoretischen Teil entsprechend die Lücken des folgenden Textes.

Das Szenaro

Ihr Unternehmen möchte einen zweiten Standort in einer anderen Stadt eröffnen. Um mit den Kolleg*innen an diesem Standort gemeinsam Projekte bearbeiten zu können, gibt es den Plan, bestimmte Daten auf einen Cloud -Speicher hochzuladen, so dass diese von beiden Standorten bearbeitet werden können. Weil Sie sich gut mit dem Thema auskennen, beraten Sie die Kollegen dazu, worauf Sie im Unternehmen achten sollten.

Lückentext

Ein Cloud-Service funktioniert im Grunde so, dass uns ein Dienstleister seine Rechnerinfrastruktur zur Verfügung stellt. Über das _____ können wir auf dessen Rechnerkapazitäten zugreifen. Dort können wir dann entsprechend die _____ nutzen, die wir für unsere Projekte benötigen. Die E-Mail-Adressen unseres Unternehmens sind zum Beispiel auch ein _____, weil sie auf einem Server beherbergt sind, der uns nicht selbst gehört, sondern auf dem wir _____ und Rechenleistung mieten. Wenn unsere Unternehmens-Webseite nicht auf einem _____ beherbergt ist, der uns selbst gehört, dann basiert auch die Webseite auf einem Cloud-Service. In der Cloud kann unser Unternehmen aber nicht nur Inhalte ablegen und verwalten, die öffentlich sichtbar sind, wie unsere Webseite oder unser Online-Webshop.

Es können auch Anwendungen und Software in der _____ zur Verfügung gestellt werden, die wir intern benutzen wollen. So einen Dienst nennt man auch _____. Ein gutes Beispiel hierfür ist die Bearbeitung von Dokumenten online. Bei vertraulichen _____ sollten wir genau darauf achten, ob der Cloud-Anbieter in seinen _____ angibt, ob er auf unsere Inhalte zugreifen kann und ob diese verschlüsselt werden. Manche Anbieter verschlüsseln alle Inhalte, andere haben Zugriff auf alles, was auf ihren Servern beherbergt wird. Wenn der Cloud-Anbieter die Inhalte unverschlüsselt speichert, könnte unser Unternehmen sich damit behelfen, vertrauliche Daten selbst zu _____, bevor wir sie online in der Cloud speichern. Das ist wichtig, um die Daten vor einem _____ zu schützen. Bei der Sicherheit sollten wir allerdings nicht nur an Angriffe denken, sondern auch an Unfälle und Pannen. Es ist deshalb wichtig, dass der Cloud-Anbieter unserer Wahl regelmäßig unsere Daten sichert, indem _____ auf einem anderen Server gespeichert werden. Wir sollten außerdem aus Gründen des _____ darauf achten, dass der Anbieter eine Auftragsdatenvereinbarung unterschreibt.

Fehlende Wörter:

Backups, Geschäftsbedingungen, Datenschutzes, Speicherplatz, unberechtigten Zugriff Dritter, Internet, Cloud-Service, Anwendungen, Server, Software as a Service (SaaS), Dokumenten, verschlüsseln, Cloud

LÜCKENTEXT L5

LÖSUNG

Ein Cloud-Service funktioniert im Grunde so, dass uns ein Dienstleister seine Ein Cloud-Service funktioniert im Grunde so, dass uns ein Dienstleister seine Rechnerinfrastruktur zur Verfügung stellt. Über das **Internet** können wir auf dessen Rechnerkapazitäten zugreifen. Dort können wir dann entsprechend die **Anwendungen; Software; Rechenleistung** nutzen, die wir für unsere Projekte benötigen. Die E-Mail-Adressen unseres Unternehmens sind zum Beispiel auch ein **Cloud-Service**, weil sie auf einem Server beherbergt sind, der uns nicht selbst gehört, sondern auf dem wir **Speicherplatz** und Rechenleistung mieten. Wenn unsere Unternehmens-Webseite nicht auf einem **Server** beherbergt ist, der uns selbst gehört, dann basiert auch die Webseite auf einem Cloud-Service. In der Cloud kann unser Unternehmen aber nicht nur Inhalte ablegen und verwalten, die öffentlich sichtbar sind, wie unsere Webseite oder unser Online; Web-Shop. Es können auch Anwendungen und Software in der **Cloud** zur Verfügung gestellt werden, die wir intern benutzen wollen. So einen Dienst nennt man auch **Software as a Service; SaaS**. Ein gutes Beispiel hierfür ist die Bearbeitung von Dokumenten online. Bei vertraulichen **Dokumenten; Inhalten; Daten** sollten wir genau darauf achten, ob der Cloud-Anbieter in seinen **Geschäftsbedingungen** angibt, ob er auf unsere Inhalte zugreifen kann und ob diese verschlüsselt werden. Manche Anbieter verschlüsseln alle Inhalte, andere haben Zugriff auf alles, was auf ihren Servern; Rechnern; Computern beherbergt wird. Wenn der Cloud-Anbieter die Inhalte unverschlüsselt speichert, könnte unser Unternehmen sich damit behelfen, vertrauliche Daten selbst zu **verschlüsseln**, bevor wir sie online in der Cloud speichern. Das ist wichtig, um die Daten vor einem **unberechtigten Zugriff Dritter** zu schützen. Bei der Sicherheit sollten wir allerdings nicht nur an Angriffe denken, sondern auch an Unfälle und Pannen. Es ist deshalb wichtig, dass der Cloud-Anbieter unserer Wahl regelmäßig unsere Daten sichert, indem **Backups/Sicherheitskopien** auf einem anderen Server gespeichert werden. Wir sollten außerdem aus Gründen des **Datenschutzes** darauf achten, dass der Anbieter eine Auftragsdatenvereinbarung unterschreibt.

QUIZ Q5

Sie können das folgende Quiz alternativ auch in Form eines Online-Spiels direkt auf ihrem Smartphone oder Computer durchführen.

Das Online-Quiz ist verfügbar auf der Bottom-Up-Webseite: https://www.dsin-berufsschulen.de/unsere-online-quiz.

1. Wofür steht die Abkürzung „SaaS“?

A Sales and action Service
B System analytics and Service
C Software as a Service

2. Was muss man bei einer Ausfallsicherheit von 99 Prozent bedenken?

A Nichts. Dafür ist diese hohe Ausfallsicherheit ja da!
B Es ist zu 99 Prozent sicher, dass das System irgendwann ausfällt.
C Mit einem Ausfall des Systems an insgesamt 3,5 Tagen im Jahr wäre bei so einem Angebot zu rechnen.

3. Was ist im Zusammenhang mit der Cloud eine „Migrationsstrategie“?

A Der Versuch, mit Hilfe von Cloud-Diensten die Migration von Menschen in Europa besser zu organisieren.
B Eine Strategie, um die Unabhängigkeit eines Unternehmens vom Cloud-Anbieter zu sichern, wenn es mit seinen Daten zu einem anderen Anbieter wechseln möchte.
C Eine Strategie der Absicherung, damit im Falle der Migration eines Unternehmens ins Ausland die Cloud dahin mitgenommen werden kann.

4. Was muss bei Dienstleistungen aus der Cloud beim Datenschutz beachtet werden?

A Personenbezogene Daten dürfen nie in einer Cloud gespeichert werden.
B Der Cloud-Anbieter muss eine Auftragsdatenvereinbarung unterschreiben.
C Das Unternehmen muss dem Cloud-Anbieter einen hohen Datenschutz garantieren.

5. Was ist ein Vorteil von Cloud-Diensten?

A Man kann online von überall auf die Daten und Dienste zugreifen, nicht nur vom Bürorechner aus.
B Die Speicherung von Daten in der Cloud ist gut für die Umwelt.
C Es macht einen sehr professionellen Eindruck, wenn Unternehmen diese Technologie nutzen.

6. Was ist ein Nachteil von Cloud-Diensten?

A Man macht sich unter Umständen abhängig vom Cloud-Anbieter.
B Die Vereinten Nationen haben einer Verwendung von Cloud-Diensten keinen technischen Standard verliehen.
C Cloud-Dienste sind meistens nur auf Englisch verfügbar.

7. Was müssen Mitarbeiter*innen beachten, wenn sie Unternehmensdaten auf bisher noch nicht verwendete Cloud-Dienste übertragen wollen?

A Der Dienst sollte zuerst bezahlt werden, sonst macht sich das Unternehmen eventuell strafbar.
B Wenn bisher kein Cloud-Dienst verwendet wird, haben die Mitarbeiter*innen freie Auswahl und können zunächst verschiedene Anbieter ausprobieren.
C Sie müssen auf jeden Fall vorher Rücksprache mit dem Unternehmen / Verantwortlichen halten.

8. Die Datensicherheit in der Cloud ist...

A ... zuerst einmal schwieriger zu erreichen als bei internen Systemen, weil alle Daten online sind.
B ... generell sehr schlecht, weil alle Daten öffentlich sind.
C … zu 99 Prozent garantiert. Das ist das Geschäftsmodell von Cloud-Anbietern.

9. Was ist eine virtuelle Maschine?

A Alle Maschinen mit Visualisierungen sind virtuell: Virtual-Reality-Brillen, Bildschirme, Displays usw.
B Ein Programm, das in einem großen Rechenzentrum simuliert, dass man auf einem eigenen Computer arbeitet.
C Eine Maschine, die mit einem 3D-Drucker hergestellt wurde.

Lösung: 1 C, 2 C, 3 B, 4 B, 5 A, 6 A, 7 C, 8 A, 9 B

BOTTOM-UP:
BERUFSSCHÜLER FÜR IT-SICHERHEIT

hat zum Ziel, die Mitarbeiter von morgen bereits während der dualen Ausbildung auf die Herausforderungen des digitalen Arbeitsalltags im Hinblick auf IT-Sicherheit und Schutz von Daten vorzubereiten. Damit leistet Bottom-Up einen wichtigen Beitrag zu mehr IT-Sicherheit in kleinen und mittleren Unternehmen.

www.dsin-berufsschulen.de

Bottom-Up ist ein Angebot von

Deutschland sicher im Netz e.V.
Albrechtstraße 10
10117 Berlin

www.sicher-im-netz.de

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Im Rahmen der Initiative:
IT-Sicherheit IN DER WIRTSCHAFT

Ein Projekt von:
DsiN Deutschland sicher im Netz

Initiative „IT-Sicherheit in der Wirtschaft“ Die Initiative „IT-Sicherheit in der Wirtschaft“ des Bundesministeriums für Wirtschaft und Energie will vor allem kleine und mittlere Unternehmen beim sicheren Einsatz von IKT-Systemen unterstützen. Gemeinsam mit IT-Sicherheitsexperten aus Wissenschaft, Wirtschaft und Verwaltung soll eine Grundlage dafür geschaffen werden, um die Bewusstseinsbildung in der digitalen Wirtschaft beim Thema IT-Sicherheit im Mittelstand zu stärken. Unternehmen sollen durch konkrete Unterstützungsmaßnahmen dazu befähigt werden, ihre IT-Sicherheit zu verbessern. Weitere Informationen zur Initiative und ihren Angeboten sind unter: **www.it-sicherheit-in-der-wirtschaft.de** abrufbar.