IT-Sicherheit

Für Alternativen offen sein

[10.12.2020] Beim Homeoffice sowie beim Homeschooling muss die Datenschutz-Grundverordnung (DSGVO) beachtet werden. Das ist praktisch nicht möglich, wenn bekannte Anwendungen von US-Unternehmen genutzt werden – doch es gibt Alternativen.

Im Juli 2020 wurden viele kalt erwischt: Mitten in einer Pandemie, die viele Arbeits- und Schulplätze in die eigenen vier Wände brachte, wird das Privacy-Shield-Abkommen vom europäischen Gerichtshof (EuGH) für ungültig erklärt. Als Begründung gaben die Richter an, dass das europäische Datenschutzniveau von den amerikanischen Unternehmen nicht eingehalten werden kann. Jedoch ist bei einer Datenverarbeitung in Drittländern genau das die Anforderung. Das lässt sich nach Meinung von verschiedenen Datenschutzbehörden nicht heilen. Hintergrund sind Regularien, nach denen US-Unternehmen solche Daten an unterschiedliche Institutionen und Behörden herausgeben müssen – unter Umgehung der EU-Gesetzgebung. In der Folge kamen auch schon die ersten Abmahnungen. Bereits 101 Unternehmen wurden aufgrund von Verstößen verklagt.

Strenge Regeln für die Datenverarbeitung in Drittländern

Schon vor einigen Jahren war so das Safe-Harbor-Abkommen geplatzt. Dennoch scheint im Großteil von Europa der Eindruck zu herrschen, dass die nächste Ausnahmeregel vor der Tür steht und eine Änderung der IT-Struktur ein unnötiger Aufwand sei. Der EuGH bemängelt jetzt die Übertragung von Nutzer-, Telemetrie-, Meta- und weiteren Daten an die Server der US-Unternehmen. Die Erhebung solcher Daten kann nach der Datenschutz-Grundverordnung (DSGVO) aufgrund von Einwilligung stattfinden, jedoch wird es problematisch, wenn die Anbieter ihren Hauptsitz oder ihre Server in den USA haben. In diesem Fall gibt die DSGVO strenge Regeln für die Datenverarbeitung in Drittländern vor. Diese Regeln konnten durch das Privacy-Shield-Abkommen erfüllt werden. Nun ist die Verarbeitung von personenbezogenen Daten durch amerikanische Anbieter de facto illegal.

Öffentliche Source-Codes ermöglichen Transparenz

Die Daten, die übermittelt werden, zählen zu den personenbezogenen Daten, sie gelten somit als besonders schützenswert. Eine Verarbeitung unterliegt also strengen Richtlinien, die von der DSGVO vorgegeben werden. Nun wird immer bemängelt, dass es keine Lösungen gibt, die komfortabel und schnell sind, gleichzeitig aber über ein hohes Schutzniveau verfügen. Dadurch wird deutlich, wie hoch die Abhängigkeit von amerikanischen Unternehmen hierzulande ist. Trotz der Aussagen der EU-Kommission, die Datenhoheit zurückerlangen zu wollen, wird dieses Vorhaben bislang nicht umgesetzt. Dabei sind das Wissen und die Lösungen in Deutschland vorhanden, es muss nur Offenheit gegenüber Veränderungen bestehen.
Die bekannten Anwendungen können nach einem Lizenzerwerb sofort genutzt werden. Neben On-Premises-Lösungen bieten vor allem Abo-Cloud-Dienste wie Microsoft 365 und Google Workspace einen schnellen Einstieg. Dieser wird jedoch durch das Brechen der DSGVO erkauft. Wird eine sichere Lösung angestrebt, führt kein Weg an auf eigenen Servern installierter kommerzieller Software und Open Source Software vorbei. Die öffentlichen Source-Codes ermöglichen Transparenz und eine Kontrolle von unterschiedlichen Instanzen.

Angebot an Programmen ist vielseitig

Diese Transparenz führt dazu, dass Lücken schnell erkannt und Fehler zügig behoben werden können. Die Offenheit macht die Software auch unabhängig von einzelnen Unternehmen, Funktions- und Sicherheitsupdates können immer weiter entwickelt und veröffentlicht werden. Das Angebot an Programmen ist vielseitig. Für jede Office Suite gibt es ein LibreOffice, für jedes Zoom ein Jitsi Meet, für jedes WhatsApp oder Teams ein Element/Matrix und für jedes Outlook ein Thunderbird. Daneben existieren unzählige weitere Produktivlösungen, wie zum Beispiel Nextcloud.
Im Kern können Abo-Cloud-Dienste auch als Managed Cloud Service aufgefasst werden. Obwohl die Skepsis nicht zuletzt durch den Verlust von Daten bei Konferenzlösungen oder dem generellen Verlust des Privacy Shields gegenüber der Cloud groß ist, steigen die Nutzerzahlen stetig an. Um Sicherheitsbedenken auszumerzen, ist der Fokus auf Private Cloud Server wichtig. Im Gegensatz zu den Abo-Cloud-Diensten werden keine Public Server genutzt, sondern die Private Cloud befindet sich auf eigener Hardware, die nicht geteilt werden muss. Der schnelle, komfortable und sichere Weg ist also ein Managed Private Cloud Service. Ein deutscher Anbieter wie Cloud1X mit zertifiziertem deutschen Rechenzentrum macht das Bild komplett und gewährleistet eine 100-prozentige Compliance-Fähigkeit.

Plattformübergreifende Kommunikation

Für die tägliche Arbeit, im Büro oder in der Schule sind zum Beispiel Software-Angebote von Cloud1X Meet basierend auf Jitsi Meet und dem Messenger Element, der auf dem Matrix-Protokoll aufgebaut ist, geeignete Lösungen. Cloud1X Meet powered by Jitsi legt den Fokus auf Videokonferenzen, während Cloud1X Meet Element je nach Wunsch auf unterschiedliche Arten genutzt werden kann. In der Anwendung Element besteht auch die Möglichkeit, Unterhaltungen über Cloud1X Meet zu starten, um vom schriftlichen zum sprachlichen Austausch zu wechseln. Über Element können zudem Verbindungen zu anderen Messengern aufgebaut werden, was eine plattformübergreifende Kommunikation ermöglicht. Die von der EU-Kommission geforderte Protokoll-Interoperabilität und Offenheit kann somit schon heute in großen Teilen umgesetzt werden.
Weitere Services für Schulen und Kommunen, Tools für Verbands- und Gremiensitzungen, Streaming-Dienste und Portale runden das Portfolio ab. Wer die Zeit und den Aufwand in Kauf nehmen will, kann die Dienste auf seiner eigenen Infrastruktur hosten. Der Kosten-Nutzer-Faktor ist beim Kauf eines Managed Private Cloud Services jedoch deutlich höher, als beim Betrieb auf eigenen Servern.

Rechenzentrum im europäischen Wirtschaftsraum

Ein guter Managed Private Cloud Service kann anhand einiger weniger Faktoren identifiziert werden: Der Beauftrage ist Betreiber der Cloud Server und erhält einen Auftragsverarbeitungsvertrag (AV-Vertrag) vom Anbieter. Das ermöglicht die DSGVO-konforme Arbeit und erhöht die Transparenz. Der Anbieter verfügt zudem über mehrere Zertifikate, wie etwa ISO 27001. Das Rechenzentrum befindet sich im europäischen Wirtschaftsraum und die Server haben eine hohe Leistung. Die Bandbreite beträgt mindestens ein Gigabit, damit eine stabile Verbindung auch bei 2.000 Teilnehmern auf dem Server garantiert ist. Des Weiteren sollte geklärt werden, wie das Gesamtpaket aussieht und welche weiteren Funktionen möglich sind.
Der richtige Weg in die Zukunft ist die Nutzung von Private Cloud und Open Source Software. Das haben schon viele Landkreise in Baden-Württemberg und Bayern sowie anderen Teilen Deutschlands erkannt und sind auf Dienste von Cloud1X umgestiegen, um intern und extern einfach und sicher kommunizieren und arbeiten zu können. Statt auf neue Sonderregeln zu hoffen, ist jetzt der beste Zeitpunkt, um die Digitalisierung voranzutreiben. Die Lösungen sind da, sie müssen nur genutzt werden.

()

Dieser Beitrag ist in der Ausgabe Dezember 2020 von Kommune21 erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit, Datenschutz-Grundverordnung (DSGVO), Open Source, Private Cloud