carmasec

security. done. right.

Whitepaper 05/2020

Kollaborationsplattformen aus Sicht der Cybersicherheit - Vergleich und Best Practices

carmasec

Über das Whitepaper

Kollaborationsplattformen sind inzwischen unverzichtbare Werkzeuge in modernen Unternehmen, die ihre Wertschöpfung weniger durch Herstellung von Waren als vielmehr durch wissensintensive Tätigkeiten erzielen. Dies schließt auch Dienstleistungsaktivitäten im produzierenden Gewerbe ein. Der dezentrale Zugriff auf betriebliche Daten, ihr Austausch und ihre Bearbeitung in Echtzeit sowie die Organisation der dafür erforderlichen Kommunikation innerhalb und zwischen Teams stellen wichtige Anforderungen an moderne Arbeitsumgebungen, die durch Kollaborationsplattformen erfüllt werden können.

Mit den augenscheinlichen Vorteilen dieser Applikationen gehen gleichzeitig Risiken einher, die Unternehmen genau prüfen und bewerten müssen, insbesondere unter dem Blickwinkel der Datensicherheit und des Datenschutzes.

In diesem Whitepaper werden die Kollaborationsplattformen Google Suite, Office 365 und Atlassian Jira / Confluence aus der Perspektive der Cybersicherheit verglichen und bewertet. Denn die Inanspruchnahme eines Cloud-Dienstes, wie sie von den meisten Kollaborations-Applikationen angeboten wird, befreit anwendende Unternehmen nicht von ihrer Verantwortung, Anforderungen des Datenschutzes und der Datensicherheit einzuhalten. Am Beispiel der drei genannten Kollaborationsplattformen wird den Leserinnen und Lesern aufgezeigt, worauf Unternehmen bei der Bewertung von solchen Diensten aus Sicht der Cybersicherheit achten müssen. Damit stellt das Whitepaper eine sinnvolle und nützliche Ergänzung zu anderen Quellen dar, in welchen vorrangig der Funktionsumfang, die Integrationsfähigkeit zu anderen betrieblichen Applikationen sowie ihre Benutzerfreundlichkeit bewertet werden.

Inhalt

ZUM AUTOR

Carsten Marmulla ist Managing Partner der auf Cybersicherheit spezialisierten Beratungsboutique carmasec GmbH & Co. KG mit Hauptsitz in Essen. Als „Trusted Advisor“ ist er seit mehr als 20 Jahren Ansprechpartner für den Themenkomplex Cybersicherheit sowohl für viele mittelständische Unternehmen als auch DAX-Konzerne. Seine Branchenexpertise weist hierbei ein breites Spektrum auf. Er hat bislang Mandate in der Telekommunikation, im Bereich Medien/Entertainment, der chemischen und pharmazeutischen Industrie, in der Gesundheitsbranche, der Logistik und der Finanzdienstleistung wahrgenommen.

Herausgeber und Urheber:
carmasec GmbH & Co. KG | Ruhrallee 185 | 45136 Essen

Was sind Kollaborationsplattformen?

Ein moderner Arbeitsplatz ist für viele Erwerbstätige - ob selbständig oder in Anstellung - insbesondere in Anbetracht der aktuellen Corona-Situation, nicht mehr an einen bestimmten Ort gebunden. Dennoch müssen Dokumente, Prozesse, Fristen und Termine für alle jederzeit einsehbar und verfügbar sein. Ohnehin nimmt generell die Bedeutung von dezentraler Arbeit zu (siehe Infokasten), weil sich auch die Tätigkeitsinhalte der meisten Berufe verändert haben. Sie sind wissensintensiv, erfordern einen erhöhten Aufwand für Koordination und Kommunikation sowie eine agile und iterative Herangehensweise in der Aufgabenerfüllung, da das Arbeitsergebnis oft nicht vorhersehbar ist.

Hinzu kommt die ständig wachsende Komplexität der Aufgaben. Immer mehr Beteiligte, die nicht nur geografisch verteilt sind, sondern sich auch aus unterschiedlichen Funktionsbereichen eines Unternehmen rekrutieren, müssen in den Bearbeitungsprozess integriert werden. Des weiteren müssen unternehmensweite Applikationen beispielsweise der Buchhaltung, Arbeitszeiterfassung, Personalplanung, Customer Relationship Management sowie andere Funktionen des betrieblichen Ressourcenmanagements integriert werden.

Eine virtuelle Kollaborations-Plattform, auf der Teambesprechungen stattfinden, Aufgaben zugewiesen und ihre Erfüllung überwacht werden, Honorare freigegeben, Dokumente verwaltet und geteilt werden sowie in Echtzeit von mehreren Personen bearbeitet werden, stellt ein inzwischen unverzichtbares Werkzeug für den modernen Arbeitsplatz in einem Unternehmen dar. Während einige Plattformen sich auf die Funktion einer Teildisziplin - etwa Dokumentenverwaltung, Zeitmanagement, Ressourcenmanagement, Kommunikation, Auswertung, usw. - konzentrieren, bieten andere Produkte umfangreiche Komplettlösungen mit vielfältigen Funktionen: Aktualisierungen des Aufgabenstatus, Dateifreigaben und Fortschrittsvisualisierungen sind ebenso verfügbar wie Videokonferenzen, Live-Sharing und Whiteboard-Funktionen.

Ein wesentlicher Vorteil von Kollaborationsplattformen kann als “Wertschöpfung statt Verschwendung” zusammengefasst werden: Zweifelsohne helfen diese Softwarelösungen Unternehmen bei der Optimierung von Prozessen und dem Ressourceneinsatz von Arbeitszeit und Arbeitskraft, wenn Daten und Informationen zentral abgelegt, ausgetauscht und bearbeitet werden. Mit den augenscheinlichen Vorteilen von Kollaborationsplattformen gehen allerdings essenzielle Herausforderungen einher, die Unternehmen genau überprüfen müssen, wenn sie diese einsetzen oder ihren Einsatz ausbauen möchten. Neben Anpassungsfähigkeit, Funktionsumfang und Benutzerfreundlichkeit müssen auch **Sicherheitsrisiken wie Datenverlust, Datenklau und Datenschutz** berücksichtigt werden. Denn die Sicherheitsstandards variieren von Anbieter zu Anbieter.

WARUM WERDEN KOLLABORATIONSPLATTFORMEN IMMER WICHTIGER?

Die wachsende Bedeutung von Kollaborationsplattformen geht einher mit fundamentalen Veränderungen in den Tätigkeits- und Aufgabeninhalten der Mitarbeiter in Unternehmen: der Anteil wissensintensiver Tätigkeiten, wie sie in der Forschung und Entwicklung, im Marketing und Vertrieb, in der Unternehmenssteuerung und im Controlling sowie in vielen weiteren Abteilungen ausgeübt werden, haben immer mehr an Bedeutung für die unternehmerische Wertschöpfung gewonnen. Diese Tätigkeiten setzen oft keine physische Präsenz voraus. Wesentlich bedeutender ist, dass Teams überregional und sogar international übergreifend zusammenarbeiten müssen. Kollaborationsplattformen bilden dabei eine virtuelle Ergänzung zum physischen Arbeitsplatz und sind eine Voraussetzung, um die Aufgaben erfüllen zu können. Insgesamt kann davon ausgegangen werden, dass dezentrales Arbeiten, auch unter dem Begriff Telearbeit („remote working“) zusammengefasst, zukünftig weiter an Bedeutung gewinnen wird.

Was sind die Herausforderungen aus Sicht der Cybersicherheit?

Vorweg gesagt: In einem wesentlichen Punk macht der Einsatz von Kollaborationsplattformen aus Sicht der Cybersicherheit die Arbeit der Beschäftigten sicherer, denn sie schreiben weniger E-Mails. Dies verkleinert die Angriffsfläche für Cyberattacken erheblich, da E-Mails oft noch unverschlüsselt übertragen werden. Zugleich bergen Kollaborationsplattformen aber neue Risiken, durch die Angreifer an wettbewerbsrelevante Daten im Unternehmen gelangen können. Zum einen werden die sensiblen Informationen zentral und in manchen Fällen auf nicht-EU-Servern gespeichert. Zum anderen fehlt es in Unternehmen oftmals an nötigen Kenntnissen und Kompetenzträgern für die sichere Konfiguration dieser Dienste.

Wir verweisen an dieser Stelle auf unser zuletzt erschienenes Whitepaper zu dem Thema
Was ist neu am Geschäftsgeheimnisgesetz (GeschGehG) - aus Sicht der Cybersicherheit?

www.carmasec.com/geschgehg

Dies ist im Besonderen vor dem Hintergrund des seit April 2019 geltenden **Geschäftsgeheimnisgesetzes** ein höchst wichtiger Aspekt bei der Nutzung von Kollaborationsplattformen. Reichte es früher zum Schutz von Geheimnissen in deutschen Unternehmen aus, bestimmte Informationen und Dokumente als “geheim” einzustufen, verlangt das neue Gesetz, “angemessene Geheimhaltungsmaßnahmen” zu ergreifen und diese nachweislich zu dokumentieren, um im Falle eines Missbrauchs rechtliche Ansprüche geltend machen zu können. Denn das Gesetz sieht eine sogenannte Beweislastumkehr vor, wonach Unternehmen nachweisen müssen, dass sie ihre Daten angemessen geschützt haben. So verlangt der Gesetzgeber unter anderem einen eindeutig geregelten Zugang zu geheimen Dokumenten und Informationen, ihre nachweislich sichere Aufbewahrung und klare Regeln zum Umgang mit Passwörtern. Nicht zuletzt müssen Unternehmen verständlich dokumentierte Richtlinien und Weisungen zum Umgang mit Geschäftsgeheimnissen vorweisen, auf die alle Beschäftigten im Unternehmen zugreifen können.

Eine spezifische Herausforderung aus Sicht der Cybersicherheit besteht darin, dass die meisten Kollaborations-Applikationen Cloud-Dienste nutzen. Die Nutzung solcher Dienste birgt eine besondere Gefahr: Im Falle eines Cyberangriffs würden womöglich alle Inhalte auf der cloudbasierten Kollaborationsplattform vollständig verloren gehen. Da die Kontrolle über Daten und Geräte an Dritte abgeben wird, sind die Geschäftsmodelle solcher Unternehmen fragil und verwundbar für Angriffe. Damit wird die Frage nach der Sicherheit der in Clouddiensten abgelegten Daten relevant: Werden diese Daten verschlüsselt? Und inwiefern hat das Unternehmen Kontrolle über die Verschlüsselung dieser Daten in der Cloud?

Eine Lösung dieses Problems bietet der Einsatz so genannter Hardware Security Module (HSM). Hierbei handelt es sich um ein externes Peripheriegerät, mit dessen Hilfe Unternehmen ihre in der Cloud abgelegten Daten mit selbst generierten Schlüsseln, auf die auch der Cloud Service Provider (CSP) keinen Zugriff besitzt, schützen können. So senken Unternehmen zwar ihre Abhängigkeit von Drittanbietern, allerdings verursacht der Einsatz von HSM bei ihnen den zusätzlichen Aufwand, ein eigenes Schlüsselmanagement aufzusetzen und zu betreiben. Dies erhöht zudem die Komplexität bei der Nutzung solcher Cloud-Dienste.

Laut der Europäischen Datenschutzgrundverordnung (DSGVO) gilt der Einsatz von Cloud-Diensten als Auftragsdatenverarbeitung. Unternehmen müssen somit überprüfen, ob die Anbieter dieser Dienste die Datenschutzbestimmungen einhalten. Denn auf Kollaborationsplattformen werden beispielsweise personenbezogene Daten von Beschäftigten, Lieferanten und anderen Dritten übertragen, und ein Unternehmen muss den Schutz dieser Daten gewährleisten. Diese Herausforderung korrespondiert mit den Compliance-Anforderungen, die aus Sicht der Cybersicherheit eine weitere Herausforderung in der Nutzung von Kollaborationsplattformen darstellen.

Herausgeber und Urheber:
carmasec GmbH & Co. KG | Ruhrallee 185 | 45136 Essen

Das Risiko der Nicht-Erfüllung von **Compliance**-Anforderungen ist vielen Unternehmen nicht hinreichend bewusst. Viele Anbieter von Kollaborations-Applikationen versprechen zwar eine bessere und für den Nutzer vereinfachte Erfüllung dieser Erfordernisse. Das führt aber dazu, dass sich Unternehmen ihrer Verantwortung für die Einhaltung von Compliance-Anforderungen nicht mehr gänzlich im Klaren sind. Zum Compliance-Management im Unternehmen gehört sowohl die Aufdeckung zurück liegender als auch die Verhinderung künftiger Verstöße ebenso wie die Einhaltung der Anforderungen des Datenschutzes. Die IT muss so gestaltet sein, dass personenbezogene Daten geschützt sind. Mit Blick auf die Datenschutz-Grundverordnung (DSGVO) geht die Verpflichtung noch wesentlich weiter: Betroffene Unternehmen müssen nicht nur den Schutz der personenbezogenen Daten gewährleisten, sondern auch sicherstellen, dass Bürgerinnen und Bürger, zu denen ja auch die Beschäftigten gehören, Kontrolle über ihre personenbezogenen Daten haben.

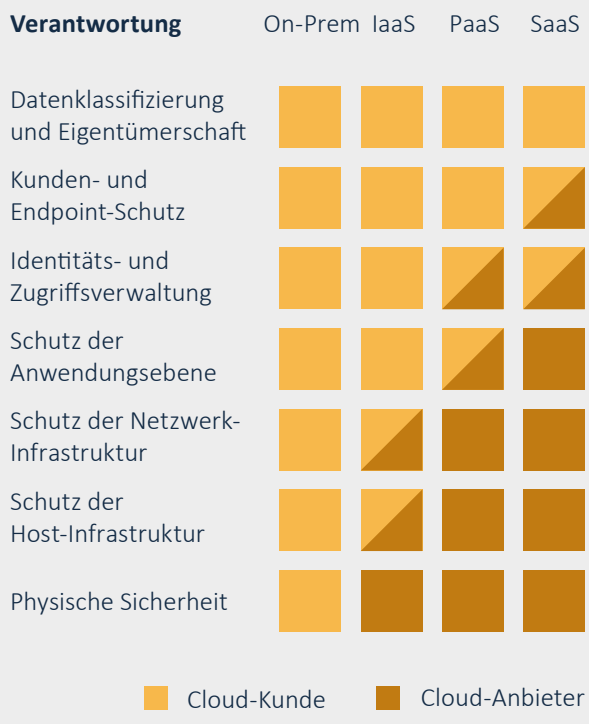
Was bedeutet das für Unternehmen, die Cloud-Dienste wie Kollaborationsplattformen im Unternehmen einsetzen möchten?

Für Cloud-Dienste existieren unterschiedliche Servicemodelle, in denen graduelle Verantwortlichkeit an das Compliance-Management in Unternehmen adressiert wird (siehe Abbildung rechts). Wer eine Kollaborations-Software auf den eigenen Servern installiert und hostet (On-Prem), ist für das Compliance-Management vollumfänglich verantwortlich. Wer diese Dienste als Software-as-a-Service (SaaS) nutzt, bleibt ebenfalls, wenn auch in geringerem Maße, verantwortlich.

Alle bekannten Anbieter von Kollaborationsplattformen weisen auf verschiedene **Konformitätsnachweise** hin, die bei den Anwendern Vertrauen schaffen sollen, beispielsweise:

- ISO 27001 (Informationssicherheit) oder der C5-Kriterienkatalog des BSI
- ISO 27017 (Cloud Security), ISO 27018 (Datenschutz in der Cloud), ISO 27701 (Datenschutz)

Insbesondere der Standard ISO 27001 ist in diesem Kontext interessant, da sich hierdurch ein Managementsystem für Informationssicherheit zertifizieren lässt. Im Gegensatz zu den beiden anderen Standards können sich Anbieter durch einen externen Auditor prüfen und zertifizieren lassen lassen. Allerdings sei hier auch erwähnt, dass das Zertifikat selbst ohne weitere Prüfung nur eine begrenzte Aussagekraft besitzt. Zum einen befreit die bloße Existenz eines solchen Zertifikats das anwendende Unternehmen nicht von seiner Pflichten im Rahmen des Compliance-Managements. Zum anderen bedeutet eine fehlende Zertifizierung nicht zwangsläufig, dass der Anbieter in Datensicherheit und Datenschutz schlechter sein muss als ein Unternehmen mit vorliegender Zertifizierung. Auch hier ist eine detaillierte Prüfung durch das Anwenderunternehmen ein Muss.



angelehnt an Transforming Government - Cloud policy framework for innovation, security, and resilience, 2015, Microsoft

carmasec

Kollaborationsplattformen im Vergleich

Anbieter für Kollaborationsplattformen erzielten 2019 alleine in Deutschland einen Umsatz in Höhe von mehr als 430 Millionen Euro. Prognosen zufolge wird der Markt kontinuierlich wachsen und 2021 ein Umsatzvolumen von fast 460 Millionen Euro vorweisen (vgl. Statista). Entsprechend groß ist auch die Zahl der Anbieter. Neben den "Alleskönnern", die eine Komplett-Lösung darstellen und für nahezu jeden Anwendungsfall geeignet sind, befinden sich auch einige Spezialisten darunter, beispielsweise "MindMeister", der mit einem Mind Mapping-Tool seit vielen Jahren im Geschäft ist, oder Zoho Projects, das im Projektmanagement breite Anwendung findet.

Wichtig an dieser Stelle: Vor einer Entscheidung für eine Kollaborationsplattform muss ein Unternehmen seine Anforderungen sorgfältig evaluieren.
Neben den Kriterien Funktionen und Benutzerfreundlichkeit gilt es, auch die erforderlichen nicht-funktionalen Anforderungen an Datensicherheit und Datenschutz zu berücksichtigen. Wichtigstes Auswahlkriterium dabei ist, inwiefern die Applikationen den Anwendern die Möglichkeit bieten, Rahmenbedingungen und Parameter zur Datensicherheit und zum Datenschutz steuern und konfigurieren zu können.

Im Folgenden werden die größten Anbieter Google Suite, Microsoft Office 365 und Atlassian Jira / Confluence unter dem Gesichtspunkt der Cybersicherheit vorgestellt.

G Suite

Was ist Google Suite?
Google Suite (G-Suite) ist eine umfangreiche Cloud-Lösung für die tägliche Arbeit. Dabei bündelt sie eine Vielzahl an Apps für die Kommunikation wie Google Mail (Gmail) und Google Meet (Nachfolger von Hangout), Apps für Terminverwaltung, wie Google Kalender, Apps für die Zusammenarbeit im Team wie Google Drive, die weitere Office-Apps wie Docs, Tabellen, Präsentation usw. umfasst.

Was sind die Stärken von Google Suite?
Google bietet eine zentrale Administrationsoberfläche, über die Sicherheitseinstellungen und -richtlinien auch für mobile Endgeräte zentral und nahtlos angepasst und verwaltet werden können, ohne dass eine separate Infrastruktur für das Mobile Device Management (MDM) erforderlich ist. Die Administration kann auf Abteilungen, Gruppen und einzelne User heruntergebrochen werden.

Was sind die Schwächen?
Zum einen ist Google mit Details zum Compliance-Status einzelner Apps zurückhaltend. Die Vielzahl der Applikationen erschwert auch den Überblick, inwieweit die Compliance Anforderungen erfüllt werden. Außerdem ist eine echte Kollaboration nur bei den Office-Apps wie Docs, Tabelle, Präsentation usw. möglich. Dies ist zwar aus Sicht der Security kein direkter Nachteil, jedoch im Vergleich zu anderen Anbietern ein Schwachpunkt.

Für wen eignet sich Google Suite?
Im Vergleich zu den Microsoft Office-Anwendungen sind Google Apps schlank und auf wesentliche Funktionen beschränkt. Google Suite empfiehlt sich für Unternehmen, die nicht auf die Bandbreite der Funktionen von Microsoft-Produkten angewiesen sind. Security-Einstellungen können hier zudem mit geringerem Aufwand verwaltet werden. Allerdings muss ein gewisses Maß an Intransparenz hinsichtlich der Erfüllung von Compliance-Anforderungen in Kauf genommen werden.

Office 365

Was ist Office 365?
Im Gegensatz zu Google Suite ist Office 365 keine reine Cloud-Lösung, sondern eine Kombination aus verschiedenen Online-Anwendungen und der Desktop-Office-Software, die bereits vielen Anwendern bekannt ist. Mit E-Mail-Serverlösung (Exchange), SharePoint und OneDrive für Zusammenarbeit, Dokumentenmanagement und Kommunikation sowie Microsoft Teams für Videokonferenzen können Anwender auf dem Computer und Smartphone bzw. Tablets im Team mit anderen zusammenarbeiten und miteinander kommunizieren.

Herausgeber und Urheber:
carmasec GmbH & Co. KG | Ruhrallee 185 | 45136 Essen

Was sind die Stärken von Office 365?
Office 365 punktet mit dem Azure/O365 Security Center, welches speziell auf die Bedarfe von Sicherheits-Administratoren und Sicherheits-Teams im Unternehmen ausgelegt ist. Diese können hierüber nicht nur Identitäten, Daten, Geräte, Apps und Infrastrukturen verwalten, sondern auch Compliance-Anforderungen zu verschiedenen Standards, wie z.B. ISO 27001, SOX und DSGVO schnell und übersichtlich überprüfen. Ferner können sicherheitsrelevante Berechtigungen samt mehrstufiger Authentifizierungen für jeden Anwender zentral verwaltet werden.

Was sind die Schwächen?
Bereits 2018 hat das niederländische Justiz- und Sicherheitsministerium Microsoft vorgeworfen, bei der Übermittlung von Telemetriedaten in die USA nicht die Anforderungen der DSGVO zu erfüllen. Zwar hat Microsoft zumindest im Fall von Office 365 ProPlus Anpassungen vorgenommen, die niederländischen Regierungsstellen lassen jedoch den Datenschutz von Microsoft-Produkten überprüfen. Diese Evaluation ist noch nicht abgeschlossen und stellt daher eine Unsicherheit dar.

Für wen eignet sich Office 365?
Aufgrund der Marktdominanz von Microsoft Office seit den frühen 1980er Jahren gehören diese Anwendungen zur täglichen Arbeit von vielen Unternehmen und ihren Beschäftigten, die im Umgang damit geübt sind. Hinsichtlich der Funktionen stellen sie einen niedrigschwelligen Einstieg in die dezentrale und kollaborative Arbeit dar. Für die Einhaltung der Security-Anforderungen braucht es Verantwortliche, die mit der Verwaltung und Steuerung der Sicherheitseinstellungen über das Microsoft Security Center vertraut sind.

ATLASSIAN

Was ist Atlassian Jira / Confluence?
Im Gegensatz zu Office 365 und Google Suite ist Jira von Beginn an eine Applikation für die Zusammenarbeit in Teams. Bereits 2002 in den Markt eingeführt, wird Jira in mehr als 122 Ländern bei über 15.000 Unternehmen eingesetzt. Jira kommt dabei hauptsächlich in der Softwareentwicklung und dort - oft in Kombination mit der Scrum-Methode - für das Workflow-Management zur Anwendung, um Prozesse zu verwalten und zu verbessern. Inzwischen etabliert sich Jira auch immer mehr in anderen Funktionsbereichen jenseits der Softwareentwicklung.
Confluence ist eine sinnvolle Ergänzung zu Jira, um beispielsweise Workflows zu dokumentieren, den Projektteams Glossare und Richtlinien bereitzustellen oder gemeinsam Berichte zu erstellen. Die Applikation ist aufgrund ihres kollaborativen Funktionsumfangs auch bei Redakteuren sehr beliebt, um technische Anleitungen zu erstellen.

Was sind die Stärken?
Eine Besonderheit des Softwareunternehmens Atlassian ist, dass Anwendungsunternehmen die Möglichkeit haben, neben einer Cloud-Lösung die Software alternativ auf eigenen Servern zu hosten. Dies bietet eine große Unabhängigkeit und ermöglicht auch die konsequente Einhaltung der Anforderungen der DSGVO und der Cybersicherheit sowie deren Steuerung. Ein weiterer Vorteil: Administratoren können Authentifikationen und Berechtigungen - mithilfe eines intuitiven, granular aufgebautem Webinterface - für so viele Benutzer, Webanwendungen und Datenserver verwalten wie nötig.

Was sind die Schwächen?
Jira lässt sich nicht vollständig in das Identity- & Access Management (IAM) des Unternehmens integrieren. Die zentrale Authentifizierung von Benutzern lässt sich in der Regel vergleichsweise einfach realisieren, die Steuerung von Zugriffsrechten auf bestimmte Bereiche oder Seiten (Autorisierung) bleibt jedoch in der Regel eine Insellösung innerhalb der Atlassian-Umgebung.

Für wen eignen sich Jira / Confluence?
Zwar ist Jira historisch gesehen eine für Software-Teams spezialisierte Kollaborationsplattform, allerdings wird sie immer mehr von Teams genutzt, deren Arbeit durch Agilität geprägt ist. Beispielsweise sind das Projekte in der Unternehmensentwicklung und im Change Management oder abteilungsübergreifende Aufgaben, wenn etwa Marketing, Vertrieb und IT zusammenarbeiten müssen, um Digital Selling- oder E-Commerce-Projekte zu realisieren.

Handlungsempfehlungen: Das müssen Sie für mehr Sicherheit tun

Wenn Sie in Erwägung ziehen, in Ihrem Unternehmen Kollaborationsplattformen sowie Videokonferenzen zu nutzen, sind laut Carsten Marmulla, dem Cybersecurity-Experten und Geschäftsführer der Beratungsboutique *carmasec*, folgende Aspekte besonders wichtig: Führen Sie eine spezifische Risikoanalyse durch! So identifizieren Sie Ihre individuellen Risiken und können methodisch sauber eine Bewertung vornehmen und letztendlich eine Anbieterauswahl treffen. Ein Risikoprofil der einzelnen Dienstleister erleichtert die Auswahl. Nutzen Sie auch die angebotenen Sicherheitsfunktionen der Plattformen und prüfen Sie die Voreinstellungen auf Konformität zu Ihren Anforderungen!

Gehen Sie strukturiert vor und treffen Sie keine unüberlegten Entscheidungen.

Hinterfragen Sie Konformitätsaussagen und Zertifizierungen der Anbieter!

Bevor Sie sich für eine Lösung entscheiden, prüfen Sie im Detail und passend zu Ihren definierten Anwendungsfällen die Eignung des Dienstleisters und hinterfragen Sie die Konformität des Anbieters. Schauen Sie bei vorhandenen Zertifizierungen in den Geltungsbereich und prüfen Sie, welche Kontrollanforderungen tatsächlich angewandt worden sind.

Überprüfen Sie die Plattformanbieter mittels geeigneter Nachfragen!

Die Adressierung konkreter fachlicher Nachfragen zum Umsetzungsgrad von geeigneten technischen und organisatorischen Maßnahmen liefert Ihnen wesentliche Erkenntnisse für die Bewertung des Anbieters hinsichtlich des Reifegrades in den Bereichen Informationssicherheit und Datenschutz.

Behalten Sie die Sicherheitskonfiguration der Plattform im Blick!

Vermeiden Sie Risiken durch fehlerhafte Implementierung: Auch bei der Auslagerung von Aufgaben an externe Dienstleister tragen Sie die Gesamtverantwortung für Ihre unternehmerischen Handlungen und sind in der Haftung.

Nutzen Sie etablierte Verfahren zur Bewertung Ihrer Risiken!

Etablierte Ansätze aus dem Risikomanagement ermöglichen Ihnen, die jeweilige Eintrittswahrscheinlichkeit und Schadenshöhe einzuschätzen, die Umsetzung geeigneter Maßnahmen auf Ihrer Seite oder beim Dienstleister vorzunehmen und somit eine Übersicht über Ihr verbleibendes spezifisches Restrisiko zu bekommen.

Carsten Marmulla empfiehlt, sich folgende Fragen zu stellen:

- Was sind meine konkreten Anforderungen und Anwendungsfälle?
- Welche Arten von Daten will ich auf der Plattform verarbeiten (ggf. geschäftskritische oder personenbezogene Daten)?
- Wie werden personenbezogene Daten beim Plattformanbieter verarbeitet, wie kann ich eine datenschutzkonforme Verarbeitung nachweislich sicherstellen?
- Welchen Dienstleister kann ich dementsprechend verwenden (Kommt ein US-Anbieter in Frage)?
- Wie sind meine Daten im Hinblick auf die typischen Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit klassifiziert?

Herausgeber und Urheber:
carmasec GmbH & Co. KG | Ruhrallee 185 | 45136 Essen

Auch technische Aspekte und Kriterien gilt es zu bedenken:

- Mit welchem Volumen und in welchem Umfang ist die Datenverarbeitung mit der Plattform geplant?
- Wieweit erfüllt die Vorkonfiguration des Anbieters bereits nicht-funktionale Anforderungen (Informationssicherheit, Datenschutz) und wie lässt sich das Sicherheitsniveau weiter steigern?
- Wie ist das Vorgehen im Falle eines Sicherheits- oder Datenschutzvorfalls? Wie läuft die Zusammenarbeit mit dem Dienstleister in dieser Situation?

Nutzen Sie die professionelle Hilfe von externen Experten!

Die Nutzung von professioneller externer Expertise zur Entscheidungsfindung ist anzuraten, da das Themenfeld komplex ist und Erfahrungswerte im Anwendungsunternehmen meist nicht vorliegen. Professionelle Dienstleister verfügen über meist langjährige Kenntnisse bei der Lösungsauswahl, -implementierung und -konfiguration und helfen Ihnen, den Überblick zu bewahren.

Der Auswahlprozess erfordert je nach Art und Umfang der jeweiligen geplanten Anwendungsfälle ein hohes Maß an Ressourcen (Arbeitszeit, Fachkenntnisse, Investitionen) innerhalb des Anwendungsunternehmens. Die frühzeitige Einbindung von externen Experten und eine möglichst detaillierte Spezifikation der (nicht-funktionalen) Anforderungen hilft Entscheidern, möglichst ressourcenschonend zu agieren und schneller produktiv zu werden.

Fazit: Datenschutzkonforme und sichere Zusammenarbeit

Kollaborationsplattformen werden immer wichtiger: Unternehmen müssen sich mit Modellen und Anbietern von Plattformen zur Zusammenarbeit auseinandersetzen und ihre diesbezügliche Strategie definieren. Unternehmen sind gefordert, sich nicht nur mit den Funktionalitäten, der Benutzerfreundlichkeit und den fachlichen Anwendungsfällen von Kollaborationsplattformen zu befassen, sondern auch mit Fragestellungen zum Datenschutz und zu den Sicherheitsfunktionen der jeweiligen Anbieter. Denn grundsätzlich gilt: Der Einsatz einer cloud-basierten Kollaborationsplattform befreit die Unternehmen nicht von ihren Erfüllungspflichten in Bezug auf nicht-funktionale Anforderungen.

Die Einhaltung von Compliance-Anforderungen wie beispielsweise dem Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) setzen Unternehmen unter Handlungsdruck, ihre Kollaborationsplattform

1. Welche regulatorischen Rahmenbedingungen existieren spezifisch für das eigene Unternehmen und die geplanten Anwendungsfälle?

2. Mit welchen konkreten Risiken ist das Unternehmen durch den Einsatz einer solchen Applikation konfrontiert?

3. Welche Maßnahmen muss ein Unternehmen umsetzen, um die Kollaborationsplattform und die darin enthaltenen Informationen und Daten zu schützen?

4. Welche technischen und organisatorischen Maßnahmen zur Erhöhung des Sicherheitsniveaus bieten die Kollaborationsplattform und der Anbieter – und welche muss das Unternehmen selbst vornehmen?

carmasec

SO UNTERSTÜTZEN WIR SIE BEI IHRER KOLLABORATIONSPLATTFORM

IT-Governance, -Risk & -Compliance

Damit Sie auf der sicheren Seite sind

Wir ermitteln für Sie, welche regulatorischen Rahmenbedingungen für Ihr Unternehmen bei der Anwendung einer Kollaborationsplattform gelten.

Dabei bewerten wir die spezifischen Risiken, um für Sie konkrete Maßnahmen festzulegen.

Security Projektmanagement

Damit Ihr Vorhaben erfolgreich ist

Wir übernehmen für Sie das Management aller Security Stakeholder und begleiten Sie bei der Einführung der Kollaborationsplattform.

So wird sichergestellt, dass alle Sicherheitsanforderungen berücksichtigt werden.

Technische Security

Damit alles richtig eingestellt ist

Wir sorgen dafür, dass Ihre Kollaborationsplattform auf die spezifischen Anforderungen Ihres Unternehmens konfiguriert ist.

Dabei führen wir Security Quick Assessments durch, damit Ihr Kollaborationsplattform schnell arbeitsfähig ist.

SIE HABEN FRAGEN? SPRECHEN SIE UNS AN

Carsten Marmulla
Managing Partner & Senior Trusted Advisor

Schwerpunkt:
IT-GRC

Jan Sudmeyer
Managing Partner & Senior Trusted Advisor

Schwerpunkt: Security Projektmanagement

Timm Börgers
Managing Partner & Senior Trusted Advisor

Schwerpunkt:
Technische Security

UNSERE KONTAKTDATEN

www.carmasec.com
contact@carmasec.com
+49 (0) 201 426 385 900
xing.carmasec.com
twitter.carmasec.com
linkedin.carmasec.com

Herausgeber und Urheber:
carmasec GmbH & Co. KG | Ruhrallee 185 | 45136 Essen

carmasec
security. done. right.

ÜBER CARMASEC

carmasec ist eine im Jahr 2018 in Deutschland gegründete Beratungsboutique im Themenfeld Cybersicherheit und Datenschutz. Als „Trusted Advisor“ bieten wir unseren nationalen und internationalen Kunden professionelle Beratungsleistungen und Lösungen in den Bereichen DevSecOps, Secure SDLC, Automatisierung von Informationssicherheitsmanagement sowie IT-GRC (Governance, Risk, Compliance).

Unser fachkundiges Expertenteam verfügt über langjährige einschlägige Beratungserfahrung, mit der wir bereits über 100 Kundenprojekte in den Branchen Telekommunikation, Logistik, Finanzdienstleistungen, Gesundheitswesen und Energie erfolgreich umgesetzt haben.

UNSERE STANDORTE

Standort Essen

carmasec GmbH & Co. KG
Ruhrallee 185
45136 Essen

Standort Köln

carmasec GmbH & Co. KG
Im Mediapark 5
50670 Köln