Cloud Collaboration

Zusammenarbeit wie auf Wolke 7

Wer heute für die Entwicklung einer Software-Lösung Kollaborationsplattformen nutzt, ist nicht nur technologisch auf der Höhe, sondern spart auch Zeit und Geld. Mit dem Vertrauen in die Cloud hapert es allerdings noch. Zu Unrecht, wie die folgenden Fakten zeigen.

→ VON VEIT HAILPERIN

DER AUTOR

Veit Hailperin
ist Sicherheitsexperte und Professional Coach sowie Projektleiter und Initiator von AdNovums Kollaborationsplattform.
→ www.adnovum.ch

Kein Zweifel: Zur Entwicklung einer passenden und stabilen Lösung müssen alle Parteien zumindest virtuell am gleichen Tisch sitzen. Doch zwischen Kunde und Anbieter klafft oft eine Informationslücke. Das führt zu Zeitverlust sowie administrativem und koordinativem Aufwand ohne Mehrwert. Wir wollen «dä Foifer und s Weggli»: Zusammenarbeit in der Cloud und keinesfalls in den Schlagzeilen stehen, weil sich ein Hacker Zugriff auf unsere Cloud verschafft hat.

GEMEINSAM ZUM ERFOLG

Weniger Missverständnisse führen zu geringeren Folgekosten, schonen die Nerven und erlauben einen schnelleren und erfolgreichen Abschluss des Projekts. Dabei hilft es, wenn alle Parteien die gleichen Werkzeuge nutzen und Transparenz herrscht. Die Lösung ist eine Kollaborationsplattform für Kunden, Anbieter und weitere Partner. Diese muss alles bieten, was für die Projektarbeit nötig ist. Wichtig sind für die Entwicklung einer Lösung nicht nur Tickets (z. B. JIRA) und Dokumentation (z. B. Confluence), sondern auch gleichberechtigter Zugriff auf den Source Code und die Entwicklungsumgebung – denn ohne Teig kein Kuchen. Die transparente Zusammenarbeit fördert das Vertrauen. Weniger Schnittstellen begünstigen den Informationsfluss und Kunde sowie Anbieter werden zu einem Team.

Für den Aufbau der Kollaborationsplattform empfiehlt sich die Verwendung von SaaS-Lösungen in der Cloud. Eine Cloud-Kollaborationsplattform bringt neben erhöhter Flexibilität auch die üblichen Capex-zu-Opex-Verschiebungen. Weitere Vorteile sind, dass der Kunde immer die neusten Features zur Verfügung hat und keinen zusätzlichen Zugang zur Infrastruktur des Anbieters benötigt.

EIN SCHÄDLICHES NARRATIV

Geschichten sind dazu da, erzählt zu werden. Manche Geschichten sind nett, andere geschäftsschädigend. Wie verhält sich das Narrativ, dass die Cloud böse und unsicher ist?

Was bedeutet Sicherheit in der Cloud? In grossen Teilen bezieht sich Sicherheit auf die genutzte Software. Diese kann Sicherheitslücken wie SQL-Injections und Logikfehler aufweisen. Diese Probleme bestehen unabhängig davon, ob die Software in der Cloud oder auf einem eigenen Server betrieben wird. Entdeckte Lücken müssen geschlossen werden. Bei der SaaS-Lösung in der Cloud werden die Fixes direkt eingespielt. Die Lücke ist behoben, bevor ein neues Release mit Fix für die On-Premises-Variante existiert.

PUNKT FÜR DIE CLOUD

Bei der On-Premises-Variante muss das Update auf Stabilität und Kompatibilität getestet werden, bevor es auf der Produktionsumgebung installiert wird. Bis dahin vergehen schnell zwei Wochen. Ab der Veröffentlichung des Updates sind behobene Lücken den Hackern allerdings bekannt – hier ist die Cloud sicherheitstechnisch im Vorteil.

Lücken betreffen auch die Infrastruktur, etwa Betriebssystem und Firewall. Dadurch entstehen Kosten für die Wartung. Die Cloud schneidet erneut besser ab: Die Infrastruktur wird vom SaaS-Anbieter gewartet. Da der SaaS-Anbieter die Infrastruktur für viele Kunden unterhält, kann er Teams in sinnvoller Grösse zur Wartung aufstellen. Eine On-Premises-Infrastruktur gleich gut zu managen wie eine SaaS-Lösung, ist für die meisten Firmen unmöglich. Auch bei Ransomware-Angriffen gewinnt die Cloud-Variante.

WIE WAR DAS NOCH GLEICH MIT DEN USA?

In der Cloud bestehen indes zwei spezifische Risiken. Das eine ist der Cloud Act, der besagt, dass Unternehmen mit Sitz in den USA den Strafverfolgungsbehörden angeforderte Daten zur Verfügung stellen müssen – unabhängig davon, wo die Daten gespeichert sind. Für den Cloud Act heisst das: Microsofts Data Center in der Schweiz sind keine Lösung und nur gut für geringere Latenzzeiten. Die Anforderung bedarf jedoch einer richterlichen Verfügung. Diese wird erteilt, sobald die USA Sicherheitsprobleme vermuten, das heisst terroristische Aktivitäten.

Wer also nicht dabei ist, Terroristen eine sichere Kommunikationsplattform zu bauen, ist ziemlich sicher. Angenommen, die NSA bekäme Zugriff auf die Kollaborationsplattform – was will sie mit dem Code oder den Tickets? Da sind keine Daten drin. Will die NSA auf das Netzwerk einer

Cloud-basierte Kollaborationsplattformen verbinden Anbieter mit Kunden und Partnern

Firma zugreifen, kann sie das auch mittels einer Zero-Day-Schwachstelle. Das zweite Risiko ist, dass Mitarbeiter des SaaS- und des Cloud-Anbieters auf den Code oder die Tickets zugreifen können. Grundsätzlich ist der Zugang eingeschränkt und muss beantragt werden. Er wird nur gewährt, wenn wir als Kunde eine Anfrage stellen, die erfordert, dass ein Mitarbeiter des SaaS- oder des Cloud-Anbieters Zugriff erhält. Bei allen seriösen Anbietern ist der Zugang zeitlich beschränkt.

SECURITY BASIERT AUF VERTRAUEN

Die wenigsten bedenken, dass jeder Sicherheit eine Form von Vertrauen zugrunde liegt. Ein Beispiel dafür ist die Verschlüsselung im Internet. Die Kommunikation wird durch ein Public Private Key Pair geschützt. Dass das Key Pair zum richtigen Server gehört, wird von einem Zertifikat bescheinigt. Die Trust Chain bestätigt wiederum die Gültigkeit des Zertifikats. Et voilà – dem obersten Zertifikat wird vertraut. Vertrauensstiftend wirkt, dass Anbieter von Komponenten für Cloud-Kollaborationsplattformen für das Aufdecken von Sicherheitslücken sogenannte Bug Bounties zahlen. Die Summen belaufen sich auf bis zu 250 000 US-Dollar für kritische Schwachstellen. Das wäre kaum möglich, wenn die Software löchrig wäre wie ein Emmentaler.

KOLLABORIEREN OHNE KOMPROMISSE

Dass die Cloud per se unsicher ist, ist so wahr, wie dass man vom Küssen schwanger wird. Die Angst vor der Cloud ist unbegründet. Entscheidend ist, die SaaS-Lösungen sicher zu konfigurieren und die regulatorischen Vorgaben einzuhalten. Denn «secure by design» ist fraglos eine Voraussetzung für eine gemeinsame Kollaborationsplattform. Wo verbergen sich weitere Risiken?

Die Praxis zeigt: Professionelle SaaS-Lösungen sind zwar «secure by default», halten einen aber selten davon ab, Passwörter im Klartext in Konfigurationsdateien zu schreiben. Um den Mehrwert der Cloud auszuschöpfen, nutzen wir die angebotenen technischen Möglichkeiten. Die Lösung in diesem Kontext ist simpel: Abhilfe schaffen entweder die bereits integrierten Vaults oder eine Zusatzlösung wie HashiCorp Vault.

ROLLENBASIERTE ZUGANGSKONTROLLE

Alle modernen SaaS-Lösungen bieten Role-Based Access Control (RBAC) an. RBAC strukturiert und automatisiert zu nutzen, ist nicht einfach. Aber oft müssen allein schon aus rechtlichen Gründen Zugangsrechte automatisiert entfernt werden können. Dies ist beispielsweise mittels einer Customer Access ID lösbar, die Kunden und weitere Partner erhalten. Die ID lässt sich mit einem «Identity and Access Management (IAM)»-System verwalten.

So braucht sich der Kunde keine Sorgen zu machen, dass ehemalige Mitarbeitende beteiligter Firmen noch auf die gemeinsame Plattform zugreifen können. 2FA und SSO sind selbstverständlich. Die sichere Entwicklung einer Software-Lösung auf einer Cloud-Kollaborationsplattform bietet dem Kunden klaren Mehrwert. Dabei weist die Cloud im Normalfall ein höheres Mass an Sicherheit auf als eine On-Premises-Lösung. Denn Sicherheit ist ein kontextueller Prozess, kein Zustand. Der schwerste Stein, der aus dem Weg geräumt werden muss, ist das falsche Narrativ. Der Rest ist sauberes Engineering. ←