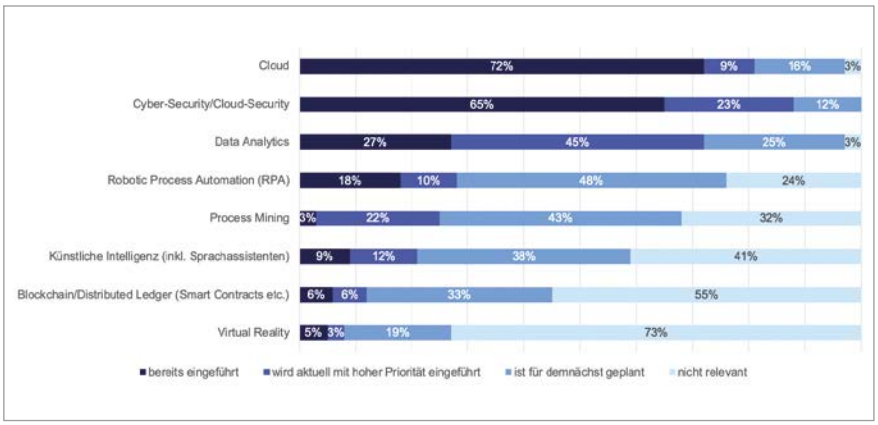
Zero Trust: Wie Banken ihre Cloud sicher machen

Gartner sagt voraus, dass der Cloud-Markt in diesem Jahr erstmals ein Volumen von mehr als 300 Mrd. US-Dollar erreicht. Dazu tragen auch die deutschen Banken einiges bei. 72 Prozent, das zeigt eine aktuelle Lünendonk-Studie, sind bereits in der Cloud oder auf dem Weg. Doch was den Schutz von Daten und IT angeht, gelten andere Regeln.

Autor:
David Schmitz,
Partner bei Senacor Technologies und spezialisiert auf Cloud-Transformation



Die wichtigsten Aufgaben der nächsten 36 Monate (Abb. 1) *Quelle: Lünendonk, Senacor*

80 Prozent der Banken in Deutschland, Österreich und der Schweiz wollen sich mit einem der großen Cloud-Anbieter zusammentun. Die Commerzbank hat sich jüngst für Microsoft Azure entschieden, wenn auch nicht exklusiv. Die Deutsche Bank setzt in den nächsten zehn Jahren auf Googles Cloud. Gemeinsam sollen sogar neue Produkte entstehen – so wichtig ist die Wolke für das Institut, aber auch die Branche insgesamt. Nichts treibt die Banken mehr um (vgl. Abb. 1). Sie setzen auf Infrastrukturen (IaaS) über Plattformen (PaaS) bis hin zu Software (SaaS) aus der Cloud, um künftig schneller am Markt zu sein, daber weniger Ressourcen einsetzen zu müssen und ihre Dienste besser zu skalieren. Doch damit das gelingt, müssen die Banken auch darüber nachdenken, wie sie ihre Cloud-Aktivitäten absichern.

Nichts und niemandem trauen

Cloud bedeutet, von überall aus online auf die wichtigsten Dienste zuzugreifen, vom Mobile Banking bis hin zum Kernbanksystem. Das Problem: Auf der digitalen Autobahn lassen sich Daten abfangen oder manipulieren. PSD2 und Schnittstellen (API) erlauben etwa sehr leicht, von außen auf die Banksysteme zuzugreifen. Wer eine API falsch konfiguriert, kann dadurch auch Unbefugten ungewollt ermöglichen, vertrauliche Daten zu stehlen oder – schlimmer noch – für finanzielle Schäden zu sorgen. Dies passiert beispielsweise, wenn die API wegen zu vieler Anfragen in kurzer Zeit ausfällt. Solche DDoS-Attacken (Distributed Denial of Service) kosten betroffene Unternehmen rechnerisch mehr als 300.000 Euro – und das für jede Stunde, in der die IT stillsteht.

Eine aktuelle IBM-Studie kommt zu dem Schluss, dass Cyberangriffe vor allem die deutsche Finanzbranche teuer zu stehen kommen. Sie weist die höchsten Schadenkosten auf. Schon ein einziges Datenleck schlägt demnach mit fast 4,5 Millionen US-Dollar zu Buche. Kompromittierte Zugangsdaten stellen zwar nach wie vor die größte Gefahr dar, doch schon an zweiter Stelle steht die Cloud. Deshalb müssen die Banken mehr investieren und sich von ihrer bisherigen Security-Architektur verabschieden. Diese basiert auf der Idee, um die kritischen IT-Systeme hohe Mauern zu ziehen und tiefe Gräben zu graben (vgl. Abb. 2). Wer hinein will, braucht die richtigen Passwörter.

Doch das System hat Lücken: Zu viele Benutzer verfügen über zu viele Rechte, Daten landen auf USB-Sticks oder in E-Mail-Anhängen und Patch-Abstände sind häufig viel zu lang.

Hinzu kommt, dass nicht zuletzt durch die Cloud kaum noch ein Unternehmen alle Daten an einem Ort verwaltet. Der „Castle & Moat"-Ansatz schlägt also gleich aus drei Gründen fehl: Dezentral verwaltete Daten, mobile Zugriffe und zunehmend offene IT-Systeme durch APIs und extern eingebundene Dienste. Statt „die eine IT" abzusichern, geht es künftig also viel mehr darum, jede einzelne Komponente für sich zu schützen. Der richtige Ansatz dafür heißt „Zero Trust", also nichts und niemandem zu vertrauen. Ein Dienst, der

„Castle & Moat"-Ansatz: Die IT ist nach außen hin abgesichert (Abb. 2). *Quelle: Cloudflare*

Zahlungen auslöst, darf deshalb auch nur genau das: Zahlungen auslösen. Jeweils andere Dienste wären dafür zuständig, Zahlungen freizugeben oder den Auftraggeber zu identifizieren. Die Idee: Wenn einer dieser Dienste kompromittiert ist, bleibt der Schaden begrenzt.

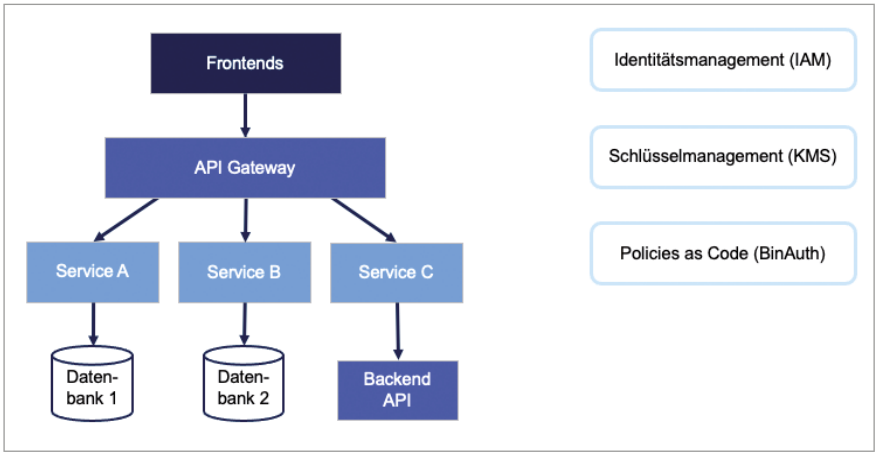
Zero Trust in die IT einführen

Weil „Zero Trust" bedeutet, sehr detailliert jede IT-Komponente zu schützen, führt kein Weg daran vorbei, die Datenströme automatisch zu überwachen. Das System muss beispielsweise merken, wenn ein Benutzer plötzlich auf eine dritte Datenbank zugreift, obwohl dieser bisher nur mit zwei anderen gearbeitet hat. Vorsicht ist auch geboten, wenn ein Zugriff statt aus dem Frankfurter Home-Office eines Mitarbeiters plötzlich aus einem Café in Manila kommt. IP-Adressen zu überwachen gehört zwingend dazu, ähnlich wie Banken das heute schon machen, wenn sie für ihre Kunden verdächtige Kreditkartenzahlungen aus dem Ausland erfassen. Drei Methoden sind unerlässlich, um „Zero Trust" in die Tat umzusetzen (vgl. Abb. 3):

1. Zugänge kontrollieren: Jeder einzelne Workload nutzt eine eigene Identität und einen eigenen Dienst-Account. IAM (Identity Access Management) regelt für jeden Dienst dessen Privilegien. Schlüssel kommen vom Key Management (KMS) und detaillierte Policies wie etwa Binary Authentification gewährleisten, dass Verbindungen aus compliancekonformen Netzen stammen.

2. Datenverkehr absichern: An jedem Kontaktpunkt müssen sich die beiden beteiligten Komponenten gegenseitig authentifizieren (mTLS). Service A kann beispielsweise nur von dazu berechtigten API-Gateways angesprochen werden. Erneut weist das KMS die Schlüssel zu und rotiert diese automatisch. Welche Dienste sich gegenseitig an- und aufrufen dürfen, regeln erneut die Policies.

3. Speicherplätze schützen: Alle Datenbanken, auch in der Cloud, sind über Schlüssel (CMEK) und Network Level Policies vor unbefugten Zugriffen geschützt. Dadurch können nur Workloads auf die Daten zugreifen, die über die richtige Identität sowie korrekte Rollen und Privilegien verfügen.



Cloud-IT: Jede System-Komponente einzeln absichern (Abb. 3). *Quelle: Senacor*

Bei diesen Vorkehrungen sollten sich die Banken nicht allein auf ihren Cloud-Provider, wie Google oder Microsoft, verlassen. Zwar verfügen gerade die großen Konzerne über eine Heerschar an Security-Experten, die viel besser als eine Bank dafür sorgen können, dass nichts schiefgeht. Eine hundertprozentige Garantie dafür gibt es aber nicht. Beispielsweise bietet sich an, eigene Schlüssel zu verwenden, statt ein vom Provider gestelltes KMS oder auf einen eigens dafür spezialisierten Anbieter zu setzen. Denn falls ausgerechnet dieser Dienst ausfällt, wären sämtliche Kunden betroffen und alle hätten auf einmal mit dem gleichen Sicherheitsleck zu kämpfen.

Fazit

In die Cloud zu wechseln, ist die richtige Entscheidung, weil die Vorteile überwiegen. Doch die Sicherheit sollte keine Bank ganz aus der Hand geben. Vielmehr erfordert die Cloud eine „Zero Trust"-Architektur, in der jeder noch so kleine IT-Baustein penibel sicher gemacht wird.

Weil es dafür keine einzelne Technologie gibt, die Banken einfach einkaufen können, müssen sie das dafür nötige Know-how aufbauen und direkt in die Software-Entwicklung integrieren. Das liegt auch daran, dass sich der Cloud-Provider nicht dagegen schützen kann, dass schadhafter Code über eine Kunden-API in die Systeme gelangt. Dafür sind die Kunden, also die Banken, selbst verantwortlich.