HashiCorp

ABN·AMRO | FALLSTUDIE

In Cloud-Sicherheit investiert

Wie eine Großbank mit HashiCorp Vault das Secrets Management automatisiert und bei wachsendem Produktportfolio enorme Einsparungen erreicht

// Innovation durch Infrastruktur

Kurzinfo zu ABN AMRO

Die ABN AMRO Bank N.V. ist die drittgrößte Bank in den Niederlanden, mit Hauptsitz in Amsterdam. ABN AMRO bietet eine breite Palette von Finanzprodukten und -lösungen für Privat-, Firmen- und Vermögenskunden an. Ihr Schwerpunkt liegt auf Nordwesteuropa. Die Bank betreut rund 6 Millionen Kunden und beschäftigt knapp 18.000 Mitarbeiter. Im Jahr 2008 wurde ABN AMRO von der niederländischen Regierung zusammen mit der Fortis Bank Nederland verstaatlicht. Seit 2015 ist sie ein öffentliches Unternehmen.

ABN AMRO FAST FACTS

> 446 Mrd. $ verwaltetes Vermögen

25 neu implementierte Plattformen

2600 Business-Anwendungen

25.000 Gesellschafter

19 Länder und Regionen

Deutlich weniger Zeitaufwand für das Onboarding von Anwendungen

Kurzlebige Secrets

> Durch die dynamischen Secrets und die API-Verschlüsselung von Vault in Verbindung mit dem Secrets Injector und sicherer Kommunikation können wir Anwendungen jetzt mit einem Bruchteil des bisherigen Zeit- und Arbeitsaufwands in unsere Container-Plattform einbinden.

TON VAN DIJK,
AGILE-PRODUKTVERANTWORTLICHER, ABN AMRO

Nur wenige Branchen erfordern ein solches Maß an Datenschutz und Sicherheit wie das Bankwesen. Und nur wenige Banken haben so weitreichende Sicherheitsanforderungen wie ABN AMRO.

Die Bank bietet ihren Kunden eine umfassende Palette von Produkten und Dienstleistungen. Doch die Sicherung der Systeme, Anwendungen und Daten, die diese Dienstleistungen erst ermöglichen, ist eine enorme Aufgabe für das 400 Mitarbeiter starke Corporate Information Security Office (CISO) des Unternehmens.

„Die Umsetzung der Zugangs- und Identitätskontrollen bei all unseren Kunden- sowie internen und externen Geschäftsanwendungen war zwar eine Herausforderung, aber mit unseren bestehenden Sicherheitslösungen zu bewältigen, selbst wenn wir Tausende neuer Konten und Benutzer hinzugefügt haben“, sagt Ton van Dijk, der bei ABN AMRO für die agilen Produkte im Bereich Identität und Zugriff zuständig ist. „Unser Bestandssystem erforderte jedoch ein zusätzliches Modul und manuelle Kontrolle, um die kurzlebigen Secrets und Schlüssel in unseren internen Anwendungen und unserer Infrastruktur zu verwalten, sodass wir beschlossen, uns nach einer nahtlosen, automatisierten Lösung für diese geschäftskritische Komponente umzusehen.“

Strategisch, sicher und stabil

Von der Finanzbranche heißt es zwar, dass sie ausschließlich auf etablierte Technologien setzt, was die Einführung neuer Lösungen oft erschwert, doch bei ABN AMRO wollte man den digitalen Wandel in Angriff nehmen, um so das Geschäft zu modernisieren und zukunftssicher zu gestalten. Eine Multi-Cloud-Strategie und die Umstellung auf Container in der Entwicklungsumgebung brachten zwar den dringend benötigten Effizienzschub für das wachsende Produktportfolio, stellten das CISO-Team aber auch vor neue Herausforderungen.

„Der Umgang mit sensiblen Daten wie Zugangsdaten oder Schlüsseln, sogenannte Secrets, ist ein geschäftskritisches Element unserer Arbeit, denn wenn eines dieser Secrets kompromittiert wird, hat das enorme Auswirkungen“, sagt van Dijk. „Schon ein einziges kompromittiertes Signaturzertifikat kann ein ganzes System lahmlegen, was bedeuten würde, dass man möglicherweise den Zugriff auf Online-Anwendungen verliert oder sie dem Risiko aussetzt, dass jemand Schadcode einschleust. Da gibt es wirklich keinen Spielraum für Fehler.“

Die bisherige Secrets-Management-Lösung der Bank hatte eine Reihe von einsatzfertigen Systemkonnektoren, die allerdings beträchtlichen Programmieraufwand erforderten, wenn eine neue Anwendung eingerichtet werden sollte. Schlimmer noch: Die selbstverwaltete Plattform lies sich nicht gut in die Kubernetes-Instanz des Teams integrierten. Also war für neue Anwendungen oder Container immer erst ein benutzerdefinierter Konnektor zu bauen. Was dazu führte, dass simple Tests einige Tage zusätzliche Vorlaufzeit benötigten.

Darüber hinaus wusste ABN AMRO, dass Secrets nicht unkontrolliert in der gesamten Umgebung verteilt werden sollten. Weil viele Anwendungen und Plattformen ihre eigenen Secrets Engines haben, ist eine zentrale Übersicht von entscheidender Bedeutung, damit Secrets im Fall einer ernsthaften Kompromittierung schnell widerrufen werden können. Wenn die Secrets über eine Vielzahl von Lösungen verteilt sind, wird die Kontrolle schwierig.

„Beim gesamten Prozess wurde uns klar, dass ein vor Ort installiertes, selbstverwaltetes Secrets-System, bei dem wir für jede Art von Änderung den Support von Drittanbietern brauchen, eine zeitraubende und ineffiziente Art und Weise ist, einen so kritischen Teil unserer Abläufe zu regeln“, berichtet van Dijk. „Es wurde von Minute zu Minute offensichtlicher, dass wir eine Cloud-native Umgebung brauchten, die Container in der Entwicklung unterstützt und auf Automatisierung ausgelegt ist – und zwar, ohne dass wir für teures Geld alles neu programmieren oder komplett neue Technologien anschaffen müssen.“

Herausforderungen

Kurzlebige Secrets sicher verwalten

Das Secrets-Management von manuellen Eingriffen befreien

Kunden-Apps und interne Anwendungen auf einen Secrets-Server ziehen

> Die Sicherheit von Daten und Systemen ist die Basis von allem, was wir tun. Mit Vault haben wir die Agilität, die Transparenz und dazu erstklassigen Support, um Lösungen für die Aufgaben von heute und morgen zu entwickeln – ohne dass wir uns Sorgen machen müssen, dass ein schlecht verwaltetes Secret unsere Arbeit zunichtemacht.

TON VAN DIJK,
AGILE-PRODUKTVERANTWORTLICHER, ABN AMRO

Zentrales Management für dynamische Secrets

Das CISO-Team von ABN AMRO wollte sein Secrets Management verbessern und unbedingt hartkodierte Anmeldeinformationen aus seinen Anwendungen und Skripten verbannen. Nach einem Proof of Concept, an dem die Fachleute aus Entwicklung und Security beteiligt waren, entschied sich das Team für HashiCorp Vault.

Mit Vault hat das CISO-Team ein zentrales Repository zur Verwaltung von Secrets implementiert, sodass die Mitarbeiter bei neuen Anwendungen und Hosts nicht mehr manuell Policies zuweisen müssen. Die Plattform funktioniert mit jeder Cloud und erleichtert die Verwaltung von Anmeldedaten und Secrets erheblich, da sie viele der sonst sehr umständlichen Prozesse automatisiert.

„Durch die dynamischen Secrets und die API-Verschlüsselung von Vault in Verbindung mit dem Secrets Injector und sicherer Kommunikation können wir Anwendungen jetzt mit einem Bruchteil des bisherigen Zeit- und Arbeitsaufwands in unsere Container-Plattform einbinden", sagt van Dijk. „Wir sind jetzt in der Lage, kurzlebige Secrets in AWS und Azure auf eine Art und Weise zu verwalten, wie wir es vorher nicht konnten – ohne zusätzliche Mitarbeiter, Kosten oder unnötig hohe Lernkurven."

Ergebnis

Reduzierung von Kosten und Komplexität durch die Abschaffung teurer Zusatzmodule

Integration von zwei Dutzend neuen Plattformen dank dynamischer Secrets

Schaffung der Grundlage für ein Encryption-as-a-Service-Modell

Lösung

ABN AMRO nutzt HashiCorp Vault und schafft damit ein zentralisiertes System zum Secrets Management für AWS, Azure und eigene Anwendungen, mit automatisierter Secrets Injection und API-Verschlüsselung. Das führt zu mehr Effizienz und reduziert kritische Fehler.

Über Ton van Dijk

Ton van Dijk ist Agile-Produktverantwortlicher bei der ABN AMRO Bank und dort zuständig für PAM (Privileged Access Management) und Secrets Management. Er ist seit 30 Jahren in der Finanzbranche tätig, nahezu ausschließlich im Bereich Cybersicherheit.

Technologie-Stack

- **Infrastruktur:** Microsoft Azure, IBM- und Cisco-Clouds on premises, Mainframe
- **Plattformen:** Windows-Server, Linux, z/OS
- **Loadbalancer:** Windows
- **API-Gateway:** Apigee, APIM
- **CA:** Managed Service von CGI (interne Zertifikate), diverse kommerzielle Anbieter
- **IAM:** SailPoint, Ping Identity (kundenseitig), PingFederate (SSO)
- **APM** (Application Performance Management): Splunk, Tivoli (on premises), Log Analytics (Azure)
- **Provisioning:** ServiceNow, Azure DevOps
- **Security Management:** HashiCorp Vault


HashiCorp