

LEITPLANKEN, KEINE SCHRANKEN

Wie ein alteingesessener, global tätiger Hersteller Compliance als Code mit Mondoo durchsetzt – bei jeder Änderung, bevor Infrastruktur überhaupt aufgebaut wird.

Interne Standards scheitern nicht, weil sie falsch sind. Sie scheitern, weil niemand sie durchsetzt. Organisationen, die Cloud-Governance als reine Dokumentationsübung behandeln, schreiben Standards, die fast niemand liest.

Diejenigen, die das Problem richtig erkennen, bauen etwas anderes: Leitplanken, die Richtlinien automatisch durchsetzen, dort wo Entwickler bereits arbeiten, ohne sie auszubremsten. Der Hersteller in dieser Fallstudie gehört zur zweiten Gruppe, und Mondoo ist die Plattform, auf der diese Leitplanken laufen.

AUF EINEN BLICK

ORGANISATION: Ein alteingesessener, global tätiger Hersteller im Transportsektor

BRANCHE: Fertigung und Transport, mit mehreren Geschäftsbereichen, darunter ein Finanzdienstleistungszweig

GRÖSSENORDNUNG: Tausende Softwareprojekte und weltweit verteilte Entwicklungsteams, die in Tausende separate Cloud-Projekte ausliefern

UMGEBUNG: Cloud-Infrastruktur, definiert in Terraform, ausgeliefert über CI/CD-Pipelines in GitHub; ein Active Directory mit Millionen von Identitäten

ENGINEERING-MODELL:

Autonome, hochgeschwindige Teams, die ihre eigene Infrastruktur besitzen – keine Change-Control-Boards

ROLLE VON MONDOO: Policy-as-Code-Durchsetzung in jeder CI-Pipeline, die Terraform gegen unternehmensspezifische Standards prüft, bevor Infrastruktur aufgebaut wird



01

DAS UNTERNEHMEN

EIN TRADITIONELLER HER- STELLER MIT EINER MODERNEN ENGINEERING-ORGANISATION

Trotz seines Images als traditionelles Industrieunternehmen betreibt dieser Hersteller eine bemerkenswert moderne Engineering-Organisation. Tausende unabhängige Teams entwickeln und betreiben ihre eigenen Anwendungen – von Bestellsystemen in der Lieferkette und Zeiterfassungssystemen bis hin zu kundenorientierten Produkt-APIs. Jedes Team besitzt seine eigene Infrastruktur, die in Tausende separate Cloud-Projekte ausgeliefert wird, und liefert mit hoher Geschwindigkeit, ohne schwergewichtige Change-Control-Boards oder aufwändige Sicherheitsprüfungen.

Diese Autonomie ist eine bewusste Strategie, und sie funktioniert. Doch sie schuf ein wachsendes Problem: Wenn jedes Team selbst entscheiden kann, wie seine Infrastruktur aussieht, entscheidet es auch darüber, wie sicher – oder unsicher – diese Infrastruktur ist.

02

DIE HERAUS- FORDERUNG

FREIHEIT OHNE LEITPLANKEN

Das Unternehmen hatte interne Standards festgelegt: Eine Produktionsdatenbank sollte Replikation und Backups haben; eine Entwicklungsinstanz nicht; Service-Accounts sollten keine überprivilegierten Cloud-StandardEinstellungen nutzen; Instanzen sollten passend zu ihrer Umgebung dimensioniert sein. Das Team nennt dies “kleines c”-Compliance – kein externes Framework wie SOC 2 oder ISO 27001, sondern die eigene Definition des Unternehmens, wie seine Infrastruktur aussehen sollte. Wie die meisten internen Standarddokumente wurden sie kaum gelesen, und nichts setzte sie durch.

Die Folgen waren real und teuer:

Ausfälle: Eine einzige Fehlkonfiguration legte einst ein kritisches Bestellsystem lahm, das von Geschäftspartnern des Unternehmens genutzt wurde. Da Bestellungen zum Stillstand kamen, stoppten die nachgelagerten Abläufe der Partner, und sie wandten sich an alternative Lieferanten – Umsatz war

schlicht verloren. Ausfallzeiten in Produktionsstätten kosten Millionen von Dollar.

Verschwendung: Entwicklungsumgebungen mit produktionsreifer Replikation, überdimensionierten Instanzen und Terabytes an unnötiger Datenspeicherung summierten sich zu erheblichen, vermeidbaren Cloud-Ausgaben.

Risiko: Teams verwendeten wiederholt Standard-Cloud-Service-Accounts mit faktisch root-artigen Rechten – ein bekanntes Anti-Pattern, das das Cloud-Team als weit verbreitet vermutete, aber nicht nachweisen konnte.

WARUM DAS VORHERIGE TOOL VERSAGTE

Das Unternehmen hatte bereits Richtlinienprüfung mit einem populären Open-Source-Infrastructure-as-Code-Checker versucht. Er lief unternehmensweit – und erreichte fast nichts, aus zwei Gründen.

Erstens konnte er unternehmensspezifische Richtlinien nicht abbilden: Seine integrierten Regeln spiegelten generische Best Practices der Branche wider, aber das Unternehmen brauchte die Durchsetzung seiner eigenen Best Practices – seinen Datenbankstandard, nicht einen Checkbox-Standard.

Zweitens blockierte er nie etwas: Befunde verschwanden in Tausenden von Seiten an Build-Logs, während die Pipelines grün blieben. Entwickler sahen nie ein Problem, also änderte sich nichts.

03

DIE LÖSUNG

POLICY AS CODE, DURCHGESETZT DORT, WO ENTWICKLER ARBEITEN

Das Unternehmen führte Mondoo in jede CI-Pipeline ein. Jede Softwareänderung im gesamten Unternehmen läuft nun durch Mondoo, das den Terraform-Code prüft, der die Infrastruktur aufbaut – und Fehlkonfigurationen erkennt, bevor sie jemals die Produktion erreichen, integriert in den bestehenden Workflow. Entscheidend ist, dass die Frameworks und ihre Kontrollen als nachvollziehbarer Code in die Plattform eingebaut sind, sodass

keine Zuordnungstabellen erstellt und keine Ableitungen manuell dokumentiert werden müssen.

INDIVIDUELLE RICHTLINIEN, VERFASST VON EXPERTEN

Fachteams verfassen ihre eigenen Richtlinien. Das Datenbankteam – der erste größere Anwender – hat rund ein Dutzend Richtlinienpakete geschrieben, die jede im Unternehmen genutzte Datenbanktechnologie abdecken: etwa 20 Prüfungen für PostgreSQL, einen ähnlichen Satz für BigQuery und so weiter. Richtlinien greifen kontextabhängig: Wenn ein Pull-Request eine Postgres-Datenbank erzeugt, läuft genau die Postgres-Richtlinie gegen diesen Code.

“ Wir sagten, Produktionsdatenbanken müssen Replikation haben. Ist das so? Zum ersten Mal kann das Datenbankteam die Antwort in einer einzigen Ansicht sehen – über Tausende von Cloud-Projekten hinweg.”

- TECHNOLOGIEVERANTWORTLICHER,
CLOUD-INFRASTRUKTUR-TEAM

FEEDBACK DORT, WO ENTWICKLER ARBEITEN

Wenn ein Entwickler – vielleicht in Indien, während das Plattform-Team in den USA schläft – einen Pull-Request öffnet, der gegen eine Richtlinie verstößt, wird die Pipeline sofort rot, in GitHub, in ihrem bestehenden Workflow. Kein Scanner-Portal zu erlernen, kein Ticket zu erstellen, kein Sicherheitsteam involviert. Sie lesen den Befund, korrigieren das Terraform, pushen einen Commit, und die Pipeline wird grün. Sie haben sich selbst zurück in die Leitplanken korrigiert, in ihrer eigenen Zeitzone, mit minimalem Geschwindigkeitsverlust.

AUSNAHMEN MIT INFORMIERTER ZUSTIMMUNG

Auf Unternehmensebene hat jede Regel legitime Ausnahmen – vielleicht benötigen 20 von Tausenden Projekten tatsächlich Replikation in der Entwicklung. Der bisherige selbstgebaute Ausnahmeprozess des Unternehmens war ein verwirrendes Geflecht interner Webanwendungen. Mit Mondoo beantragen Entwickler Ausnahmen direkt in der App, und Anfragen werden automatisch an den richtigen Fachexperten weitergeleitet: Datenbank-Ausnahmen gehen an das Datenbankteam, Cloud-Plattform-Ausnahmen an das Cloud-Team. Das anfragende Team genehmigt niemals seine eigene Ausnahme, und jede Entscheidung hinterlässt eine Prüfspur. Nach Genehmigung läuft die Pipeline erneut und wird grün.

EIN ANTRIEBSMECHANISMUS FÜR ALTLASTEN

Dies ist keine grüne Wiese – es ist so “brownfield”, wie es nur geht. Das Ziel war nicht nur,

neue Verstöße zu verhindern, sondern auch, jahrzehntealte, angesammelte Konfigurationsschulden stetig abzubauen. Die CI-Durchsetzung erledigt dies automatisch: Wird ein ruhendes Repository aus irgendeinem Grund berührt – selbst nur ein Tippfehler in einer README –, markiert Mondoo jeden bestehenden Verstoß in diesem Projekt, bevor die Änderung gemergt werden kann. Probleme lösen sich mit der Zeit von selbst, ohne dass jemand einen Sanierungs-Backlog zuweisen muss.

04

SKALIERUNG & INTEGRATION

GEBAUT FÜR ECHTE UNTERNEHMENSGRÖSSE

Die Integrationsanforderungen waren extrem. Das Active Directory des Unternehmens enthält Millionen von Identitäten – jeder, der jemals in irgendeiner Funktion mit dem Unternehmen zu tun hatte. Neue Mitarbeiter gehören am ersten Tag Hunderten von Gruppen an, was Annahmen sprengt, die in Standard-Identitätsprotokollen verankert sind. Die rollenbasierte Zugriffskontrolle musste absolut dicht sein: In einem Unternehmen, in dem Sicherheitsdaten auf ein noch nicht angekündigtes Produktprogramm hinweisen könnten, dürfen Personen nur sehen, wofür sie verantwortlich sind.

Die gesamte Mondoo-Bereitstellung wird zudem zu 100 % über Terraform verwaltet – ohne einen einzigen Klick –, einschließlich Identitätsintegration, Organisationsstruktur und Workspace-Layout. Die Struktur unterstützt eine übergeordnete Unternehmensrichtlinie mit kontrollierter Autonomie der Geschäftsbereiche: Der Finanzdienstleistungszweig, der fast wie ein eigenständiges Unternehmen operiert, kann eigene, strengere Anforderungen über die Unternehmens-Basisrichtlinie legen, kann diese aber niemals außer Kraft setzen. Die vollständige Unternehmensintegration wurde in weniger als einem Jahr realisiert.

“ Mondoo ist der schnellste Anbieter, mit dem wir je zusammengearbeitet haben – der einzige, der vollständig in alle unsere Systeme integriert ist. Wir haben es mit riesigen Anbietern zu tun, die uns gesagt haben, dass sie das seit Jahren nicht geschafft haben.”

- TECHNOLOGIEVERANTWORTLICHER, CLOUD-INFRASTRUKTUR-TEAM

05

ERGEBNISSE

70,000+

CI-Scans pro Monat – ein Projekt wird etwa alle 30 Sekunden gescannt

3,800+

Softwareprojekte mit Infrastrukturcode entdeckt und unter Richtlinien gebracht

22,000

Richtlinienbefunde behoben

LEITPLANKEN, DIE FUNKTIONIEREN

Die Durchsetzung wurde erst vor kurzem aktiviert, und die frühen Daten zeigen, dass das Modell funktioniert. Ein Softwareprojekt wird rund um die Uhr etwa alle 30 Sekunden auf Compliance geprüft. Rund 31.000 Scans markierten Verstöße, die unter dem alten Tooling unsichtbar geblieben wären [Zeitraum zu bestätigen: 28 Tage vs. gesamte Laufzeit]. Aktive Befunde bleiben konstant, während Behebungen steigen – selbst während weitere Richtlinien ausgerollt werden. Diese Auseinanderentwicklung der beiden Linien ist das Kennzeichen wirksamer Leitplanken: Neue Verstöße werden bereits an der Quelle verhindert, während Altlasten stetig behoben werden.

Ebenso wichtig: Das Unternehmen behielt, was ihm am wichtigsten ist. Teams liefern weiterhin mit hoher Geschwindigkeit, bestimmen weiterhin selbst über ihr Schicksal und sitzen weiterhin nie vor einem Change-Control-Board.

Die Leitplanken ersetzen Bürokratie, nicht Autonomie.

06

DAS FAZIT

 mondoo.com

 email

 [linkedin](https://www.linkedin.com/company/mondoo)

STANDARDS KÖNNEN NICHT NUR GESCHRIEBEN WERDEN. SIE MÜSSEN DURCHGESETZT WERDEN.

Dokumentation ist die Grundlage; Durchsetzung an der Quelle, fortlaufend und in großem Maßstab, ist das, was Infrastruktur wirklich verändert. Dieser Hersteller ist der Beweis, dass das Policy-as-Code-Betriebsmodell in einem echten Brownfield-Unternehmen funktioniert – Tausende autonome Teams, Millionen Identitäten, jahrzehntealte Konfigurationsschulden – ohne ein einziges Change-Control-Board. Mondoo verwandelt interne Standards in Leitplanken und Leitplanken in Ergebnisse. In dieser Reihenfolge.