

DevOps



DevOps, aber sicher

Entwicklung und Betrieb von Software zu integrieren ist ein erklärtes Ziel jeder DevOps-Initiative. Angesichts der Komplexität dieser Aufgabe klammern viele Unternehmen die Sicherheit erst einmal aus. Doch das ist ein fataler Fehler.

Von Oliver Köth, NTT Data

Ist es wirklich sinnvoll, die beiden Silos Entwicklung und Betrieb auch noch mit der hermetischen Welt der Security zu einer agilen Organisation zu verschmelzen? Bedeutet das nicht, den agilen Schwung von DevOps gleich wieder auszubremsen? Zugegeben, Fragen wie diese verstehe ich als CTO eines IT-Dienstleisters nur zu gut. Schließlich geht es bei der Digitalisierung um schnelle Ergebnisse. Um Systeme, die schnell eingeführt und effizient zu betreiben sind. Doch was bringt es, wenn die Entwicklung zwar in Rekordzeit abgeschlossen scheint, das Produkt dann jedoch in Sicherheitstests durchfällt? Die Erfahrung zeigt: Neben hohen Kosten und verpassten Umsatzchancen schadet ein solcher zu spät gescheiterter DevOps-Ansatz auch der agilen Strategie, die dahintersteht. Zwar erschwert es die agile Organisation, von Anfang an Entwicklung, Sicherheit und Betrieb als ein Ganzes zu etablieren. Sicherheitsprobleme ersticken manch hoffnungsvolle Entwicklung im Keim. Doch auch hier heißt es, frühzeitiges Scheitern als Chance zu begreifen, die teure Fehlinvestitionen erspart. Die Frage ist also nicht, ob DevOps zu DevSecOps wird, sondern wie das gelingen kann.

Die Hindernisse auf dem Weg zu einer DevSecOps-Organisation unterscheiden sich kaum von denen, mit denen jeder DevOps-Ansatz ohnehin zu kämpfen hat: Neben der Silo-Struktur, die sich durch organisatorische Maßnahmen ändern lässt, ist es die verfestigte Silo-Kultur, die in den Köpfen weiterlebt. Noch stärker als im Zusammenspiel von Entwicklung und Betrieb treten dabei die Gegensätze zwischen „kreativen, aber chaotischen“ Entwicklern und „kompromisslosen, pedantischen“ Sicherheitsexperten zutage. Die gute Nachricht für alle Beteiligten: Verständigung ist möglich! Tatsächlich zeigt die Erfahrung, dass teamorientierte Zusammenarbeit zwischen Entwicklern, Administratoren und Sicherheitsexperten schneller bessere Ergebnisse hervorbringt und gleichzeitig mehr Spaß macht.

Die wichtigste Aufgabe beim Implementieren einer DevSecOps-Struktur liegt in der Führungsetage.

Sie muss Kultur-Broker etablieren, die Veränderung wollen, Gleichgesinnte finden und andere dafür begeistern können. Zunächst ist deshalb ein offener Austausch im bestehenden Rahmen erforderlich, der die Konfrontation zwischen beharrenden und änderungswilligen Kräften nicht scheut. Hier finden sich die Akteure, die gemeinsam Strukturen der gegenseitigen Anpassung und Verbindung entwickeln. Konkret geht es darum, Fragen zu stellen. Nicht um die „richtigen“ Antworten zu erhalten, sondern um den Diskurs in Gang zu bringen: Wie können IT und Business gemeinsam bestehende Prozesse verbessern und neue schaffen? Was müssen die bisherigen Silos dazu übereinander wissen? Wie können wir mit DevSecOps schneller mehr erreichen?

Diversität im Team ist ein Schlüssel für erfolgreiche agile Organisationen. Doch wie agieren interdisziplinäre Teams, wo jahrelang jede Abteilung für sich gearbeitet hat? Trotz aller Bekenntnisse zu Security by Design prallen in den meisten Unternehmen mit Development und Security auch heute noch zwei Welten aufeinander. Bei der Fusion dieser Welten zu einer agilen Organisation haben sich die folgenden praktischen Schritte bei DevSecOps-Projekten von NTT Data weltweit bewährt:

- Security-Champion-Programm installieren
- Sichere Entwicklung macht mehr Spaß
- Spezialisten für Entwicklung und Sicherheit im jeweils anderen Fachbereich hospitieren lassen
- Gegenseitiges Kennenlernen fördert das Verständnis der gemeinsamen Aufgabe
- Trainingsangebote bereitstellen
- Menschen wollen lernen – gemeinsam lernen fördert gemeinsamen Erfolg
- Verhältnis von IT und Business fair gestalten
- Mit zunehmender Digitalisierung passt die alte Einteilung in IT als Lieferant und Business als Kunde nicht mehr
- Gemeinsame Ziele setzen, dazu gehört auch, dass die DevSecOps-Teams gemeinsam entscheiden können.



Oliver Köth
ist CTO bei NTT Data Deutschland.

DevOps (Development und IT Operations) gewinnt in der Softwareentwicklung zunehmend an Bedeutung – auch im SAP-Umfeld. DevOps ermöglicht es Unternehmen, auf die sich schneller ändernden Marktanforderungen agil zu reagieren.

Bitte beachten Sie auch den Community-Info-Eintrag auf Seite 74

NTT Data
Trusted Global Innovator

