DEVSECOPS: MEHR FREIHEITEN – MEHR VERANTWORTUNG

DIGITAL Trust.

In der Anwendungsentwicklung ist vieles anders – auch die Security-Philosophie. Unternehmen stehen vor der Herausforderung, ihre vorhandenen Konzepte und Prozesse mit den Anforderungen von Entwickler-Teams zu verbinden. Denn mit modernen Entwicklungsmethoden ändert sich nicht nur die Infrastruktur, auch für die Gewährleistung der Security ist ein neuer Ansatz erforderlich: Die Security-Abteilung ist nicht mehr allein verantwortlich und muss von Beginn an bei Entwicklungsprojekten beteiligt sein.

So wird Security zum Enabler und wahrt die Balance zwischen agiler Bereitstellung und Sicherheit. Das macht neue Denkweisen und Prozesse, aber auch Know-how über die Container-Plattform und Tools erforderlich, welche die Anforderungen bestmöglich erfüllen. Wir sprechen dann von DevSecOps.

NEUE ROLLEN FÜR ANWENDER:INNEN UND SECURITY-ABTEILUNG

DevSecOps benötigt eine geteilte Verantwortung: Anwendende erhalten mehr Freiheiten und übernehmen gleichzeitig mehr Verantwortung.

So wird die Security-Abteilung zur zentralen „Security-Steuerungseinheit", welche die grundlegenden Rahmenbedingungen (Guardrails) vorgibt, aber den Nutzer:innen Entscheidungsspielräume innerhalb dieser Vorgaben einräumt. Basis hierfür ist eine enge Zusammenarbeit Ihrer Abteilungen. Keine leichte Aufgabe, denn die Sichtweisen sind oftmals sehr unterschiedlich.

UNSER VORGEHENSMODELL

Computacenter begleitet Sie in diesem Prozess. Wir unterstützen unsere Kunden bereits seit vielen Jahren bei der Absicherung ihrer Entwicklungsumgebungen und sprechen die Sprache ihrer Security-, Entwicklungs- und Ihrer Betriebsexpert:innen. Wir verfolgen einen Security-Ansatz, der ihre vorhandenen Vorgaben und Tools berücksichtigt und Empfehlungen von Cloud und Container-Umgebungen in Ihre Sicherheitsvorgaben integriert.

IHR DEVSECOPS-WEG

Als herstellerunabhängiger Partner entwickeln wir gemeinsam mit Ihnen funktionale, moderne IT-Architekturen. Dazu erstellen wir ein Sicherheitslagebild und reviewen Ihr Regelwerk.

Wir erarbeiten mit Ihnen Guardrails für die Container Security, die grundlegende Sicherheitsvorgaben mit dem notwendigen Entscheidungsspielraum für Nutzer:innen verbinden. Darüber hinaus erstellen wir Handbooks für Anwender:innen und vermitteln in Trainings, wie diese die Guardrails einhalten und welche Lösungen sie nutzen können.

Zielgenau evaluieren wir, welche Lösungen etwaige Lücken am besten schließen und erstellen technische Konzepte, welche konkreten Lösungen in der Unternehmensumgebung implementiert werden.

Sie profitieren dabei von dem spezifischen Fachwissen unserer Security-Expert:innen, gepaart mit der langjährigen Erfahrung zu Entwurf, Aufbau und Absicherung von IT-Umgebungen.

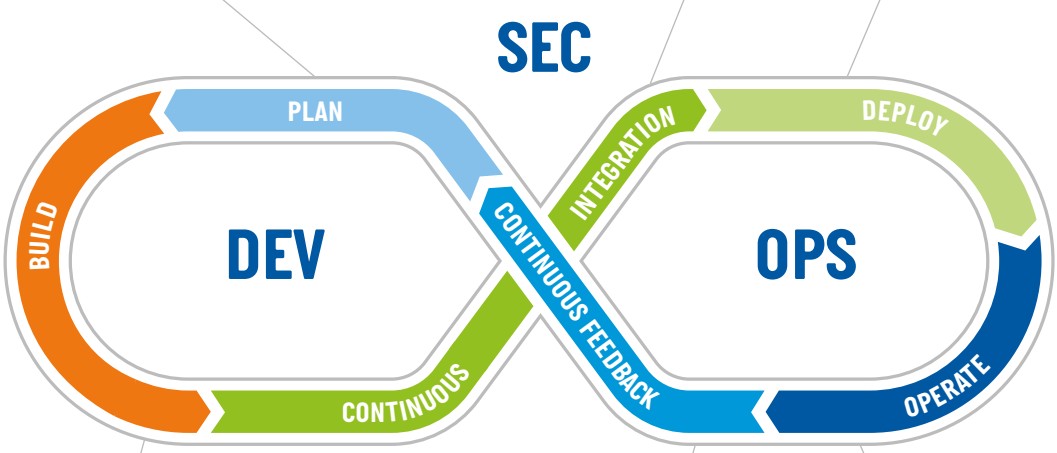
„Unser Sicherheitskonzept bietet Ihnen den Mehrwert eines umfassenden Security-Governance-Modells, das Sicherheitslösungen für Multi-Cloud- und Container-Umgebungen umfasst, sich auf eine große Partnerlandschaft erstreckt und moderne Lösungsansätze integriert."

Hauke Moritz
Solution Manager Cloud Security

- Cloud Security Framework
- Threat Modelling
- Processes & Methods
- Data Classification

- Embedded CI/CD Scanning
- Secret Management
- Software Signing
- Automated Security Solutions

- Automated Adjustments
- Code Review
- In-App Security



- Network Security
- Identity & Lifecycle Management
- Privileged Account Management
- Storage & Data Protection
- Access Management

- Vulnerability Management
- Audit & Compliance
- Penetration Testing
- Risk Assessments

- Runtime Protection
- DDoS Protection
- Cyber Defence Services
- Log Management

Computacenter

Computacenter AG & Co. oHG
Computacenter Park 1, 50170 Kerpen

Sie möchten mehr erfahren?
Sprechen Sie gern Ihr Account Management
an oder kontaktieren Sie uns über
www.computacenter.com/de