ROHDE&SCHWARZ
Make ideas real

Rohde&Schwarz Cybersecurity

SECURITY-AS-CODE

Der Schlüssel zu DevSecOps

INHALT

„Unternehmen setzen auf Cloud-Computing und Infrastructure-as-Code (IaC), um die digitale Transformation voranzutreiben – und um wettbewerbsfähig zu bleiben, denn eine Optimierung des Time-to-Market ist immer gut. Schwachstellen sind dabei eine große Herausforderung: Je später eine Schwachstelle entdeckt wird, desto teurer der Fix. Wir empfehlen Unternehmen daher einen völlig neuen Ansatz – den des DevSecOps – Security-as-Code ergänzt DevOps um Security.

Security sollte eine transparente Angelegenheit zwischen Entwicklern, Operations und Sicherheitsexperten sein – und DevSecOps nicht dergestalt verstanden, dass Sicherheit nur bei „Sec“ implementiert würde. Bei Security-as-Code wird Security möglichst nah am Quellcode in die DevOps-Toolchain und -Workflows implementiert und der Code so bereits bei der Erstellung gestärkt.

Möglich wird das durch die Einbindung automatisierter Sicherheitsrichtlinien, Tests und Scans in jeder Phase der CI/CD-Pipeline. Sie können Fehler so kontinuierlich identifizieren und direkt beheben und Developer sparen Zeit und Aufwand, wenn sie Bugs vor den Releases beheben.

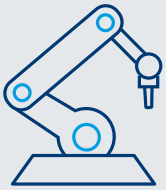
In dieser praktischen Handreichung haben wir alles Wissenswerte über Security-as-Code und wie DevSecOps Ihrem Unternehmen zum Erfolg verhelfen kann zusammengefasst. Zur leichteren Nutzung finden Sie viele praktische Listen, die Ihnen To-dos und wertvolle Vorteile einfach aufbereitet zeigen.

DAS „EVERYTHING-AS-CODE“-PARADIGMA

Wenn Sie mit Configuration-as-Code und IaC vertraut sind, sind Ihnen Security-as-Code oder Security-by-Design sicher bereits bekannt.

Seit den DevOps-Anfängen ebnet IaC den Weg für Automatisierung und verringert Risiken und Betriebskosten in der Betriebsphase.

ALLES AUTOMATISIEREN



Sicherheitstests mit Tools wie SAST, DAST und IAST sind Ihr wichtigstes Mittel zur Sicherung der Anwendung in der CI/CD-Pipeline. Automatisieren Sie den Einsatz dieser Sicherheitstools, um sie im Tandem einzusetzen – mit der Geschwindigkeit von DevOps.

1. **IaC hilft Ihnen, die Skalierbarkeit der Anwendung in einem Cloud-Ökosystem zu nutzen.**
   Es ermöglicht eine bessere Ausrichtung auf den Lebenszyklus der Anwendung.

2. **Configuration-as-Code ist ein weiteres Best Practice, bei dem Sie die Konfiguration der Anwendungsumgebung durch eine Orchestrierungs-API und Skripte beschreiben.**
   Menschliche Einflussgrößen (Fehler) im System werden reduziert und Zeit gespart.

3. **Security-as-Code baut nun auf den Vorteilen der beiden oben genannten Konzepte auf, indem die Sicherheit möglichst nah am Quellcode auf einfache, reproduzierbare und automatisierbare Weise implementiert.**
   Wie der Name schon sagt, definieren Sie dabei die Sicherheit in einer einfachen Konfigurationsdatei als Code.

UND WIE LÄSST SICH SICHERHEIT ALS CODE IN DER PRAXIS UMSETZEN?

Wichtig ist zu verstehen, dass die DevSecOps-Transformation nicht nur einen Wechsel der Tools, sondern auch eine Veränderung der Kultur erfordert.

SICHERHEITSBEWUSSTSEIN

Jeder sollte sich der Kosten bewusst sein, die Sicherheitsverletzungen für Unternehmen bedeuten, die erst spät entdeckt werden. Entwickler und Operations sollten die Verantwortung für die Sicherheit übernehmen und in sicherem Coding geschult werden.

1. **Bewerten Sie all Ihre derzeitigen DevOps-Bemühungen.** Führen Sie ein Audit Ihrer Infrastruktur durch und zeichnen Sie die aktuellen Prozesse auf, einschließlich Codeänderungen. Während des Audits ist es wichtig, Änderungen an den Sicherheitsrichtlinien zu verfolgen, um zu verstehen, wer wann welche Änderung vorgenommen hat.

2. **Mitglieder Ihres Sicherheitsteams, die sowohl die Anforderungen der Anwendung als den Kontext verstehen, sollten die Möglichkeit erhalten, einen Teil der Sicherheitsrichtlinien zu entwerfen.** Teammitglieder müssen miteinander kommunizieren, um sich abzustimmen, wenn eine Codezeile geändert oder neuer Code eingeführt wird, um zu besprechen, wer Zugang zu welchen Ressourcen hat, wie der Code von der Commit- zur Produktionsphase gelangt, welche Tests durchgeführt werden, welche Tools verwendet werden.

3. **Ihre leitenden Developer und das Betriebsteam müssen in sicheren Kodierungspraktiken geschult werden.**

4. **Ernennen Sie einen Sicherheitsbeauftragten in Ihrem DevSecOps-Team, der Sie über die verschiedenen Sicherheitskonzepte auf dem Laufenden halten kann.**

5. **Automatisieren Sie Ihre Continuous-Delivery-Pipeline so weit wie möglich.**

6. **Führen Sie automatisierte Sicherheitstests an allen anfälligen Punkten des Prozesses durch und fügen Sie so eine weitere Sicherheitsebene zu den in der Produktion verwendeten Code-Review-Tools.**

WARUM IST SECURITY-AS-CODE WICHTIG FÜR IHR DEVSECOPS-TEAM?

Security-as-Code spielt bei Ihrer DevSecOps-Transformation eine große Rolle, da es Ihnen hilft, Security zu verlagern und den Prozess dank Automatisierung zu vereinfachen. Weitere wichtige Vorteile sind die Förderung der Kollaboration, Agilität und die Verbesserung der Transparenz zwischen Development-, Operations- und Securityteams.

Sicherheitsengpässe werden verringert und die Einhaltung von Aufsichtsstandards stattdessen gewährleistet. **Und je sicherer Ihre Anwendungen sind, desto besser lassen sie sich verkaufen!** Daher ist Security-as-Code das Rückgrat von DevSecOps und ermöglicht es Developern, sich auf ihre Stärken zu konzentrieren, ohne dabei die Security aus den Augen zu verlieren.

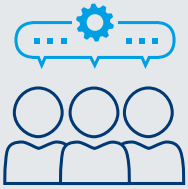
3 TIPPS FÜR EINE ERFOLGREICHE SECURITY-AS-CODE-KULTUR

1. **Einfache Implementierung:**
   Das Ziel sollte sein, neue Prozesse an bereits bestehende interne Prozesse des Unternehmens anzupassen. Dies ermöglicht Ihnen mehr Steuerung und Agilität.

2. **Intensive Kollaboration:**
   Bauen Sie ein Sicherheitsteam auf, das die Sicherheitspolitik im Unternehmen global überwacht und sich Aufgaben mit dem DevSecOps-Team teilt. Ein solcher Managementansatz harmonisiert die Arbeit von Developern und Security, was zu insgesamt optimierter Performance führt.

3. **Effektive Messung:**
   Exakte, effektive Metriken, die auf Kosten und Gewinne abzielen, sind unerlässlich. Dank dieser Indikatoren kann ihr Team das optimale Ressourcenniveau und Erwartungen in Bezug auf erzielte Werte definieren.

SILOS BESEITIGEN



Developer-, Operations- und Sicherheitsteams müssen eine Vision teilen, um einen Kulturwandel zu fördern. Multikompetente und kleinere Teams sind wesentlich flexibler und effektiver. Agiler Input der Teammitglieder und ihr Engagement in jeder Phase ist entscheidend.

9 TAKTIKEN ZUR ERHÖHUNG DER SECURITY – GARANTIERT OHNE NEGATIVE EFFEKTE AUF MARKTEINFÜHRUNG UND INNOVATION

Als Unternehmer müssen Sie die Markteinführungszeit und das Innovationsniveau gegen einen entscheidenden Faktor abwägen – Anwendungssicherheit. Ungenügende Layer-7-Security kann Ihr Gesamtziel, ein optimales Kundenerlebnis, beeinträchtigen. Das Streben nach Innovation und Geschwindigkeit führt zwangsläufig zu Sicherheitsbedrohungen. Es ist dabei eine falsche Vorstellung, Sicherheit ginge zwangsläufig auf Kosten von Agilität und Innovation.

Wir möchten Ihnen aufzeigen, wie DevSecOps das perfekte Modell sein kann, um Ihre innovativen Anwendungen in der „Security-as-Code"-Ära schnell auf den Markt zu bringen.

Rohde&Schwarz Cybersecurity verfügt über das Know-how, die Prozesse und Werkzeuge, die Sie unterstützen, von der Security-as-Code-Kultur zu profitieren. Die Markteinführung von R&S®Trusted Application Factory, einer modernen, cloud-basierten Lösung zum Schutz von Anwendungen, verdeutlicht unsere Mission, Anwendungen von morgen zu schützen.

Der Schlüssel liegt im Erreichen von Interoperabilität im CI/CD-Bereich. Und, da es sich um eine tool- und technologieunabhängige Lösung handelt, lässt sie sich mühelos in Ihre CI/CD-Pipeline integrieren.

ALLES MESSEN

Zuverlässige Sicherheits-KPIs und OKRs in einem zentralen Dashboard sind der Schlüssel zu richtigen Entscheidungen und Entscheidungen. Sie helfen Ihnen, den Zustand Ihrer Infrastruktur zu visualisieren und die Gesamtkosten gut zu planen. Die Auswertung von Kennzahlen hilft bei der Einhaltung der Datenschutzgrundverordnung (DSGVO) und vermeidet hohe Strafen durch die Beseitigung von Datenlecks.

Wie können Sie also Security mit DevSecOps nutzen und gleichzeitig Innovation und schnelle Markteinführung realisieren?

1. **Verkürzen Sie die Release-Zyklen:**
   Inkrementelle Zyklen sorgen dafür, dass Sie mit den sich ändernden Anforderungen der Kunden Schritt halten. Kurze, häufige Release-Zyklen helfen, Code in kleineren Fragmenten zu analysieren, Lücken zu identifizieren und sichere Anwendungen schneller bereitzustellen.

2. **Automatisieren Sie so viel wie möglich:**
   Sie müssen die Sicherheit an mehreren Stellen in die CI/CD-Pipeline integrieren, denn manuelle Sicherheitsprüfungen oder die Konfiguration von Sicherheitskontrollen können zeitaufwändig sein. Wenn die von primären Sicherheitstools wie SAST, DAST und SCA gefundenen Probleme zu groß sind, können Sie diese mit cloud-nativen Anwendungsschutzlösungen kombinieren, um Ihre Anwendungen schneller zu schützen. Darüber hinaus können Sie durch die automatisierte Bereitstellung der Anwendung und der zugehörigen Sicherheitslösung Zeit gewinnen.

3. **Probleme früher angehen:**
   DevSecOps ist eine Erweiterung von DevOps, bei der Sie den Schwerpunkt auf die Sicherheit in frühere Phasen verlagern. Je früher Sie eine Schwachstelle finden, desto einfacher und kostengünstiger ist es, sie zu beheben. Das Aufspüren und schnelle Patchen einer Schwachstelle, sobald sie gefunden wird, verringert nicht nur Ihr Sicherheitsrisiko, sondern sorgt auch für eine insgesamt schnellere Bereitstellung der Anwendung.

   Sie fragen sich, wie effizientes Virtual Patching Ihre Ergebnisse verbessern kann?

4. **Verwalten Sie Schwachstellen mit Bug-Bounty-Plattformen:**
   Nicht alle Unternehmen sind in der Lage, Schwachstellen rechtzeitig zu erkennen. Bug-Bounty-Plattformen bieten eine gute Alternative. White-Hat-Hacker dafür zu bezahlen, dass schwerwiegende Fehler in Anwendungen aufzuspüren, anstatt später von böswilligen Akteuren ausgenutzt zu werden, kann Geld und Reputation sichern.

5. Förderung einer engeren Zusammenarbeit:

Eine optimierte Markteinführung hängt also von einer Kulturveränderung und den richtigen Tools ab. Aber auch der Faktor Mensch in DevSecOps-Team ist relevant. Ihre Sicherheitschampions fördern letztlich gemeinsame Verantwortung in den verschiedenen funktionsübergreifenden Teams. Es gibt verschiedene Ansätze zur Integration der Teams. Solche integrierten Bemühungen tragen zu einer einfachen Bereitstellung und kürzeren Markteinführungszeit bei.

6. Setzen Sie auf Container und eine auf Mikrodiensten basierende Infrastruktur:

Native Cloud-Technologien sind dynamisch, leicht zu skalieren und aus der DevOps-Perspektive einfach zu warten. Wenn Developer mehr Anwendungen unter Einsatz von Microservices bauen, können sie menschliche Einflussgrößen (Fehler) vermeiden, wertvolle Zeit sparen und die Wettbewerbsfähigkeit steigern.

7. Verwaltung von WAF-Fehlalarmen:

Sie sollten die Verwaltung von Fehlalarmen früher in den Erstellungsprozess und nicht erst zu Beginn der Betriebsphase einbinden, denn False Positives sorgen für einen hohen Ressourcenverbrauch. Die Zeit für Sicherheitsüberprüfungen wird verkürzt, wenn Geschwindigkeit und Qualität der Identifizierung von False Positives erhöht wird.

8. Bereitstellung in SaaS:

SaaS-Modelle schaffen eine Win-Win-Situation. Sie verkürzen nicht nur die Markteinführungszeit, sondern bieten Skalierung. Da die Anwendungen in der Regel in der Cloud gehostet werden können, entfällt der Aufwand für Softwareverwaltung.

WEITERE INFORMATIONEN

R&S®Trusted Application Factory bietet verkürzte Markteinführungszeit verbunden mit erstklassiger Security. Kontaktieren Sie uns, um eine Demo zu vereinbaren.

dev-appsec.rohde-schwarz.com

Rohde & Schwarz Cybersecurity
Rohde & Schwarz Cybersecurity ist ein führendes IT-Sicherheitsunternehmen, das digitale Informationen und Geschäftsprozesse von Unternehmen und öffentlichen Institutionen weltweit vor Cyberangriffen schützt. Der IT-Sicherheitsexperte bietet innovative Datensicherheitslösungen für Cloud-Umgebungen, erweiterte Sicherheit für Websites, Webanwendungen und Webservices sowie Netzwerkverschlüsselung und Endpoint-Sicherheit. Die vertrauenswürdigen Sicherheitslösungen werden nach dem Security-by-Design-Ansatz entwickelt und verhindern Cyberangriffe proaktiv.

Rohde & Schwarz
Der Elektronikkonzern Rohde & Schwarz bietet innovative, Lösungen in folgenden Geschäftsfeldern: Messtechnik, Rundfunk- und Medientechnik, Sichere Kommunikation, Cybersicherheit sowie Monitoring and Network Testing. Vor mehr als 80 Jahren gegründet, ist das selbstständige Unternehmen mit seinem Firmensitz in München in über 70 Ländern mit einem engmaschigen Vertriebs- und Servicenetz vertreten.

Rohde & Schwarz Cybersecurity GmbH
Mühldorfstraße 15 | 81671 München
Info: +49 30 65884-222
Email: cybersecurity@rohde-schwarz.com
www.rohde-schwarz.com/cybersecurity

Rohde & Schwarz GmbH & Co. KG
www.rohde-schwarz.com

PD 3683.4210.61 | Version 01.00 | September 2021 (sch)
Security-as-Code
Titelbild: © www.istockphoto.com - Cecilie_Arcurs

3683.4210.61 01.00 PDP 1 de
368342 1061