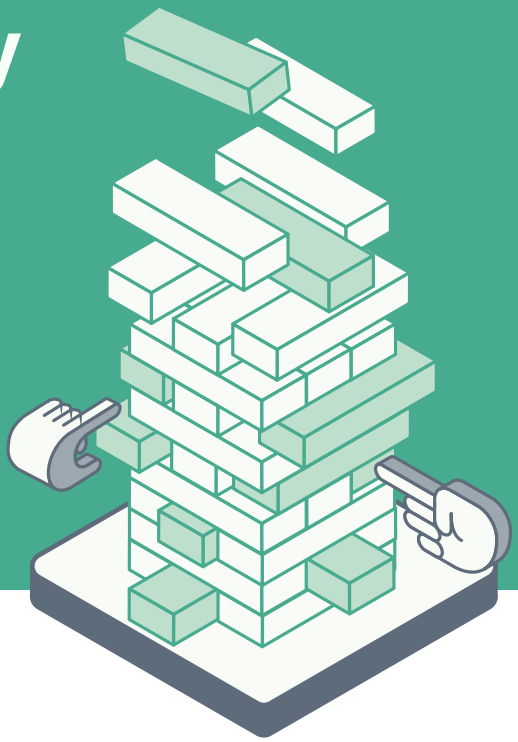
Supply Chain Security in der Finanzbranche

Ein Unternehmen aus der FinTech-Branche setzt bei der Entwicklung digitaler Applikationen für Endkunden sowohl auf Inhouse-Ressourcen als auch auf externe Zulieferer und Projektteams. Um vor dem Go-live neuer Lösungen einen Compliance-konformen Security-by-Design-Ansatz zu etablieren, wurden die Experten von Cloudyrion als Partner für IT-Sicherheit ins Boot geholt.



AUSGANGSLAGE

Angriffe auf die Supply Chain bereiten Cybersicherheitsexperten seit vielen Jahren Sorgen, da die Kettenreaktion, die durch einen Angriff auf einen einzigen Lieferanten ausgelöst wird, ein ganzes Netz von Anbietern gefährden kann. Malware ist die vorherrschende Angriffstechnik, die bei 62 Prozent der Angriffe eigesetzt wird. Laut dem ENISA-Bericht Threat Landscape for Supply Chain Attacks, in dem 24 aktuelle Angriffe analysiert wurden, reicht eine starke IT-Security für Unternehmen nicht mehr aus, nachdem die Angreifer ihre Aufmerksamkeit bereits auf die Zulieferer verlagert haben. Dies zeigt sich an den zunehmenden Auswirkungen dieser Angriffe: Ausfallzeiten von Systemen, finanzielle Verluste und Rufschädigung.

Aktuellen Prognosen zufolge werden sich die Angriffe auf die Lieferkette im Jahr 2021 im Vergleich zum Vorjahr vervierfachen. Dieser neue Trend unterstreicht die Notwendigkeit zu handeln für Unternehmen und ihre Entscheider. Es gilt, dringend neue Schutzmaßnahmen einzuführen, um potenzielle Angriffe auf die Supply Chain in Zukunft zu verhindern, bei Bedarf angemessen zu reagieren.

Entwicklung
Die zunehmende Bedrohung durch die Einschleusung von bösartigem Code macht es erforderlich, internen Code und strukturelle Abhängigkeiten gezielt abzusichern – in Open-Source- ebenso wie in kommerziellen Tools. Das Durchsickern von Geschäftsgeheimnissen oder anderen sensiblen Daten und die Manipulation von Code vor der Veröffentlichung sind die Folgen einer kompromittierten Software-Build- und -Delivery-Pipeline. Softwareentwicklungsleiter sollten daher mit ihren Sicherheits- und Risikobeauftragten zusammenarbeiten, um die Unversehrtheit von internem und externem Code durch Durchsetzung strenger Versionskontrolle zu gewährleisten. Gängige sicherheitswirksame Empfehlungen sind zum Beispiel die Verwendung von Artefakt-Repositories für vertrauenswürdige Inhalte und das Management von Herstellerrisiken während des Lebenszyklus der Bereitstellung sowie die Sicherung von Geheimnissen und Signierung von Code und Container-Images.

Anwendung
Im konkreten Fall erwies es sich bei umfangreichen Development-Projekten von Softwareanwendungen und Services für Endkunden immer wieder als große Herausforderung, unterschiedliche Delivery-Pipelines der verschiedenen beteiligten Teams zu koordinieren. Insbesondere die automatisierte Erkennung von Schwachstellen und schadhaftem Code war angesichts der Vielzahl beteiligter Instanzen mit unterschiedlicher Awareness für das Thema ein schwer lösbares Unterfangen.

Supply Chain Security
Das Ziel: ganzheitliche Supply Chain Security einzurichten, die von der Entwicklung bis zum Endanwender keine Sicherheitslücken offenlässt, über die Systeme und Prozesse kompromittiert werden könnten. Das gewünschte Risk Management sollte die Pipeline-Security inklusive aller Tests und Tools, die dort eingesetzt werden, ebenso einbeziehen wie die Sicherheit während der Nutzung der Applikation in der Praxis (Runtime). Durch Empfehlungen auf Basis positiver Erfahrungen wurde das Unternehmen auf Cloudyrion aufmerksam und nahm Kontakt zu den Spezialisten für IT-Sicherheit mit Sitz in Düsseldorf auf. Überzeugt hat der Security-Dienstleister vor allem mit einem Ansatz, der umfassende Beratung, technologische Expertise und lösungsorientierte, pragmatische Hilfestellungen für Anwender kombiniert.

CHALLENGE

Benötigt wurde ein systematischer Security-by-Design-Ansatz, mit dem sich sicherstellen lässt, dass die von vielen internen Entwicklern und Zulieferern produzierte Software frei von Sicherheitslücken und Malware ist und den Endkunden zur Verfügung gestellt werden kann. Beauftragt wurde Cloudyrion, den Prozess von der Entwicklung bis zum Praxiseinsatz unter dem Security-Aspekt zu optimieren und mit Governance zu untermauern, um die Produkte für Endkunden sowie Enterprise-Kunden sicherer zu gestalten. Eine zentrale Vorgabe bestand darin, nach drei Monaten den Stand der sogenannten Minimum Valuable Security zu erreichen.

Die Herausforderungen:

- **Technologische Vielfalt, d.h. uneingeschränkte Funktionsfähigkeit in einer Hybrid Cloud-Umgebung**
- **Schnelle Software Release-Zyklen und unzureichende Pipeline Software Guardrails für Application- und Infrastructure-as-Code**
- **Regionale Distanz der Teams**
- **Compliance-Anforderungen (gemäß GDPR bzw. EU-DSGVO und PCI-DSS)**
- **Unsichere und stark segmentierte Continous Integration / Continous Deliver (CI/CD)-Tools**

LÖSUNG

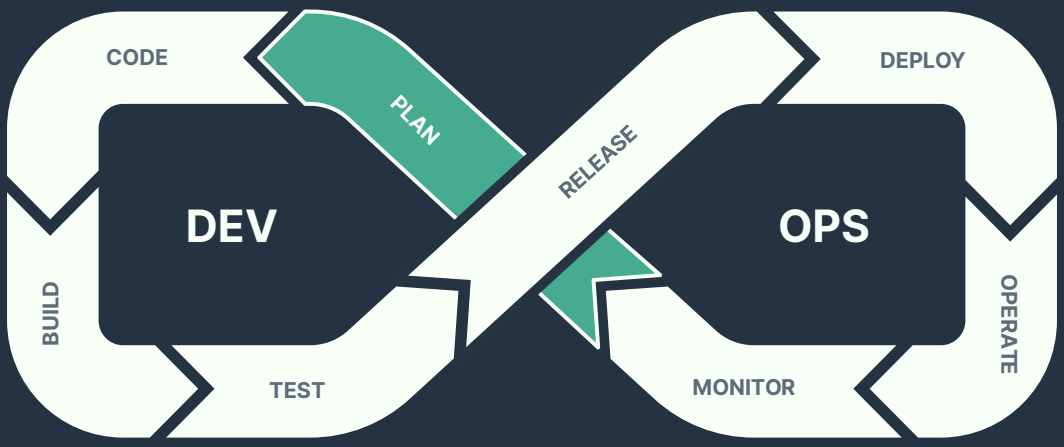
Am Anfang erfolgte ein detailliertes Threat Assessment: Cloudyrion identifizierte gemeinsam mit den jeweils beteiligten Teams potenzielle Angriffsvektoren sowie Angreifer und Risikoszenarien. Beispiele an der Schnittstelle zwischen Auftraggeber und Lieferanten sind die lückenlose Überprüfung von:

- **Single Sign-On-Integration**
- **IPS-Systemen**
- **Web Application Firewalls**
- **Identity & User Access Management: Vergabe von Zugriffsrechten und konsistente Rollenverteilung aufseiten der User**
- **Zertifikaten wie z.B. ISO, PCI-DSS etc.**

Auf Basis der Ergebnisse wurden das Design der Security-Infrastruktur angepasst und die entsprechenden Maßnahmen implementiert, um die aufgedeckten Gefahren wirksam auszuschließen. Als besonders kritisch entpuppte sich schon früh der gesteckte Zeitrahmen für das Projekt. Mit Beginn des Security-by-Design-Prozesses nahm die iterative Umsetzung entscheidender Projektschritte Fahrt auf, damit einem sicheren und Compliance-konformen Go-live nach drei Monaten nichts im Weg stand.

Im Projektverlauf entschied sich der Auftraggeber, das Verfahren zu verlängern, um über die erreichten Mindestvorgaben hinaus die Angriffsfläche kontinuierlich zu verringern und die Security Maturity schrittweise immer weiter zu erhöhen. Die wichtigsten To-Dos für Cloudyrion im Überblick:

- **Entwicklung einer gemeinsamen Strategie mit dem Kunden sowie Definition und Terminierung von Zielen**
- **Gezielte Unterstützung der Teams bei der Einführung von SCA, DAST oder IAST in ihre Pipeline und bei der richtigen Interpretation der Resultate**
- **Detailliertes Prozessdesign für die Entwicklungsphase, inklusive Definition von Risk Based Pipelines (Guardrailes)**
- **Empfehlung eines Trusted Container Registry-/Software Code Repository-Ansatzes; Hintergrund: Zu viele Tools mit gleichen Funktionen verkomplizieren das Deployment. Zentralisierung mit genehmigten Tools führt zu standardisierten und kontrollierten Deployments**
- **Härtung der CI/CD-Umgebung hinsichtlich Security**
- **Evaluation des Sicherheitslevels von externen Software Zulieferern**



AUSBLICK ZUKUNFT

Entsprechend den Anforderungen und auf Wunsch des Unternehmens stand Cloudyrion den Anwendern nach dem Go-live über die drei Monate hinaus weiterhin beratend zur Seite. Hier zahlte sich vor allem aus, dass es den Security-Consultants zuvor gelungen war, den Anwendern das erforderliche Know-how zu vermitteln, um häufig auftretende Standardfragen während der Runtime souverän selbst zu lösen. Die Folge: Vorwiegend bei außergewöhnlichen Problemstellungen wurden die Experten immer noch konsultiert, beispielsweise bei der Auswahl und Implementierung einer zuvor nicht vorhandenen SCA-Enterprise-Lösung. Dieses strategische Vorgehen hat sich bewährt und empfiehlt sich auch für etwaige künftige Projekte außerhalb des Segments Supply Chain Security.

NUTZEN UND BEURTEILUNG

„Wie bei vielen unserer Kunden haben wir auch hier besonders positives Feedback erhalten für unsere Fähigkeit, pragmatische Lösungen im Kontext des Projekts zu finden und umzusetzen – und eben nicht mit der branchenweit gefürchteten ‚Security says no'-Haltung zu Werke zu gehen", erklärt Okay Güler, Founder & IT Security Consultant von Cloudyrion. „Geschätzt wird unsere Flexibilität, mit der wir die Leute vor Ort unterstützen, Awareness für das Thema IT-Sicherheit zu entwickeln und nachhaltig in den Prozessen zu verankern."

Zentrale Ergebnisse im Überblick

- **Höheres Security Level bei Services für Endanwender**
- **Beschleunigung von Go-to-market-Timelines**
- **Schnelleres und sicheres Deployment von Versions-Updates**
- **Offenlegung von Strategie-Gaps aufseiten des Unternehmens**
- **Deutlich verbesserte Awareness und Know-how-Transfer im Bereich Security**

Sie suchen nach einem verlässlichen Partner, der Ihr Team dabei unterstützt, ehrgeizige und sicherheitskritische IT-Projekte erfolgreich umzusetzen und langfristige Verfügbarkeit zu gewährleisten? Kontaktieren Sie uns – wir helfen gern.