Rapid7 Germany
Am Söldnermoos 17
85399 Hallbergmoos
Deutschland

Konaktieren Sie uns:
+49 89 97 007 007
sales-dach@rapid7.com
rapid7.com

Anwendungssicherheit
Wer breiter testet, testet besser

Die explosionsartige Zunahme der Apps in den letzten Jahren ist geradezu phänomenal. Nach der Untersuchung von fast 5 Millionen Stunden Live-Desktop-Aktivität der Mitarbeiter des operativen Supports ergab ein Bericht von Pegasystems Inc., dass der durchschnittliche Mitarbeiter täglich mehr als 1.100 Mal zwischen 35 jobrelevanten Anwendungen wechselt. Und man kann mit Fug und Recht behaupten, dass die Cloud-Infrastruktur dies möglich gemacht hat. Sie hat unser gesamtes Denken und die Kultur unserer Arbeitsweise verändert.

Wenn wir die vergangenen Zeiten betrachten, so erforderte die Erledigung jeder Art von arbeitsbezogenen Aufgaben einen Besuch im Büro oder zumindest den Einsatz eines PCs oder mobilen Geräts mit dem richtigen VPN-Client, der darauf installiert war. Heutzutage können die Mitarbeiter auf alles, was sie zur Ausübung ihrer Tätigkeit benötigen, von so ziemlich jedem Ort aus über jedes Gerät mit einer einfachen Internetverbindung zugreifen. Von der Erstellung von Spesenabrechnungen über das Ausfüllen von Stundenzetteln und die Überprüfung von Lagerbeständen bis hin zur Möglichkeit, eine Vielzahl anderer wichtiger Funktionen zu verwalten, die den Geschäftsbetrieb aufrecht erhalten.

Und während viele Organisationen mit ihrer "Cloud-Reise" gut unterwegs sind, haben die Ereignisse der ersten Hälfte des Jahres 2020 (und wahrscheinlich auch darüber hinaus) die Dinge noch weiter beschleunigt und die Zögerlichen zum Handeln gezwungen. Die durch die globale Pandemie bedingte Auslagerung der Mitarbeiter hat zu einer noch größeren Nachfrage nach dem Zugang zu Geschäftsanwendungen geführt. Die meisten Organisationen mussten innerhalb weniger Tage einen Plan für die Heimarbeit entwickeln und umsetzen. Vorteilhaft war dabei, dass z.B. Webanwendungen hervorragend zu der neuen Betriebsumgebung passten, in der wir uns befinden. Sie sind von Natur aus plattformübergreifend, wodurch die Notwendigkeit entfällt, für jede Benutzerplattform separate Anwendungen zu entwickeln.

Applikationen werden häufig angegriffen

Doch gerade während einer Krise, wenn die Gedanken am meisten abgelenkt sind, wird das Risiko von Bedrohungen noch offensichtlicher. Und die Anwendungen scheinen das große Ziel von Angreifern zu sein. Sie sind der primäre Angriffsvektor bei Sicherheitsverletzungen: Weltweit gaben

42% der Entscheidungsträger im Bereich der Sicherheit, deren Firmen einen Angriff von außen erlebten, an, dass dieser unter Ausnutzung einer Software-Schwachstelle durchgeführt wurde. Fünfunddreißig Prozent gaben an, dass der Angriff über eine Webanwendung erfolgte.

Und das ist noch nicht alles. Ein Bericht von Verizon legt nahe, dass 43% der Verstöße Angriffe auf Webanwendungen waren, mehr als doppelt so viele wie im Vorjahr. Die Bedrohung ist sehr real:

- **Geschäftskritische Daten landen in der Öffentlichkeit:** Das heißt, Anwendungen enthalten geschäftskritische Daten und machen sie über das Internet zugänglich.
- **Exploits nutzen die Funktionalität der Anwendung:** Viele Exploits nutzen die beabsichtigte Funktionalität der Anwendung aus, so dass es sehr schwierig ist, Abhilfe zu schaffen, ohne diese Funktionalität einzuschränken.
- **Ausfallzeiten sind extrem teuer:** Die Verfügbarkeit der Anwendung ist absolut entscheidend. Viele Unternehmen führen ihre Kernprozesse über Anwendungen aus; jede Ausfallzeit kann Umsatzeinbußen bedeuten, die sich auf die Performance des Unternehmens und letztlich auf den Gewinn auswirken.
- **Die Wiederherstellung kann Jahre dauern:** Ein einziger Verstoß kann die Marke erheblich schädigen und einen CISO letztlich den Job kosten.

Kunden laufen buchstäblich davon

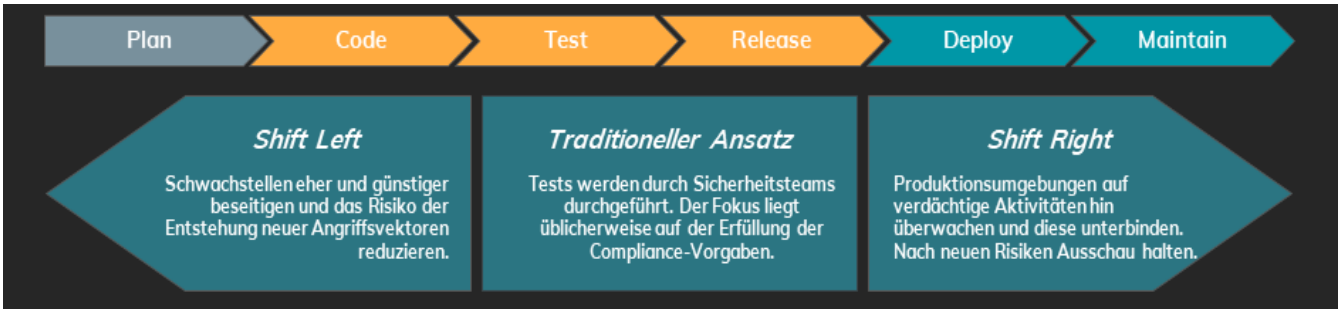
Läufer, Radfahrer und Luftfahrtexperten werden kürzlich mitbekommen haben, wie der Hersteller von Smartwatches und Wearables, Garmin, Opfer eines Lösegeldangriffs auf seine Dienste und Anwendungen wurde. Der Angriff veranlasste Garmin dazu, seine offizielle Website, den Benutzerdaten-Synchronisierungsdienst Garmin Connect, die Datenbankdienste von Garmin für die Luftfahrt und sogar einige Produktionslinien in Asien zu schließen. Während das Potenzial für Daten- und Umsatzverluste für Garmin enorm war, scheinen die Nutzer des Dienstes eher besorgt darüber zu sein, dass sie ihre letzten Aufzeichnungen nicht hochladen können. Und das ist kritisch! So werden sie unweigerlich zum nächsten Wettbewerber gehen, laufen, fahren oder fliegen.

Wenn also Anwendungen den Organisationen in einer post-pandemischen Welt Kopfschmerzen bereiten, wie kann man sie am besten schützen und die Geschäftskontinuität gewährleisten? Zunächst betrachten wir einen sicheren Software Development Lifecycle (SDLC), der beschreibt, wie Software-Teams sichere Anwendungen erstellen.

Eine Landschaft im Wandel

Traditionell haben die Sicherheitsteams Tests durchgeführt, die sich in der Regel auf die Erfüllung von Konformitätsstandards konzentrierten. Es handelt sich um einen sicherheitszentrierten Ansatz, bei dem der Schwerpunkt auf Risiko und Belastbarkeit liegt, sowohl intern als auch extern. Geschwindigkeit und Effizienz leiden jedoch darunter.

Das Konzept des "Shift Left" ist seit einiger Zeit ein beliebter Trend in der kontinuierlichen Testpraxis. Das heißt, das Testen zu einem früheren Zeitpunkt im SDLC, um Fehler billiger beheben zu können und das Risiko der Einführung neuer Angriffsvektoren zu verringern. Und obwohl dies logischerweise ein vernünftiger Ansatz zu sein scheint (und immer noch sehr wichtig ist), zeichnen sich jetzt auch Shift Right-Praktiken beim Testen als Trend ab. Auf diese Weise können sich Teams vor Problemen und Angreifern schützen, die nicht auf bekannte Exploits oder Probleme im Code setzen.



Aber wenn die Shift-Left-Mentalität schon seit einiger Zeit populär ist, warum sehen wir dann jetzt einen Trend zu Shift Right? Um das Entstehen einer "Shift Right"-Mentalität zu verstehen, muss man zunächst untersuchen, wie sich die Entwicklungsstile verändert haben. Anstelle des linearen Wasserfallmodells (populär in den 90er und frühen 2000er Jahren) ermöglicht DevOps jetzt die kontinuierliche Entwicklung und Bereitstellung von Software mit automatisierten Test- und Freigabeprozessen (im Gegensatz zu manuellen Prozessen).

Die Erwartung dabei ist, dass durch die Implementierung von DevOps alles reibungsloser abläuft, da die Software vor ihrer Freigabe automatisch auf Sicherheit getestet wird. Die Realität ist jedoch, dass automatisierte Test- und Freigabeprozesse die Sicherheit oft zugunsten von Geschwindigkeit und Effizienz vernachlässigen.

Daher erfordert die Sicherung von sich ständig ändernden Anwendungen (DevOps) eine Menge neuer Prozesse und Produktunterstützung, auf die die Dev-Teams weder vorbereitet sind noch die richtigen Tools haben, um die Sicherheit zu adressieren. Das bedeutet, dass die Sicherheit hinter das Entwicklungstempo zurückfällt. Wenn es nur eine Verschiebung nach links gibt, sind die Entwicklungsteams überlastet. Und die Statistiken lügen nicht; 47% der Entwickler sagen, dass sie nicht genug Zeit für die Sicherheit haben.

Warum Shift Right wichtig ist

Während Shift Left die Qualität und die Erfüllung der Geschäftsanforderungen sicherstellt, werden das Funktionieren und die Performance in der realen Welt durch einen Shift Right-Ansatz gewährleistet. Shift Right verwendet einen kontrollierten experimentellen Ansatz, Tests in der produktiven Umgebung und konzentriert sich speziell auf Funktionalität, Leistung, Fehlertoleranz und Benutzererfahrung. Kurz gesagt, dadurch wird sichergestellt, dass die Testteams auf reale Benutzererfahrungen reagieren können, die in der Planungsphase des SDLC oft sehr schwer zu reproduzieren sind.

Shift Right testet eine gebaute und funktionierende Anwendung, die sich bereits im Einsatz und in der Postproduktionsphase befindet. Auf diese Weise können Organisationen Feedback unter realen Bedingungen sammeln, die viel stärker auf Leistung, Benutzerfreundlichkeit und Stabilität ausgerichtet sind. Auf diese Weise wird die Qualität der Anwendung auf der Grundlage der tatsächlichen Nutzung durch die Benutzer verbessert.

Aber warum sollten Sie dies tun wollen?

Verbesserte Benutzererfahrung

Erfahrung ist im wahrsten Sinne des Wortes alles, ob Kunde oder Mitarbeiter; sie war in den letzten Jahren eine der größten Triebkräfte des Wandels. Bei der Anwendung eines Shift Right-Ansatzes werden Erfahrungen und Feedback gesammelt und dann sowohl aus geschäftlicher als auch aus technischer Sicht betrachtet. Auf diese Weise wird sichergestellt, dass alle Fragen individuell untersucht und auf dieser Grundlage verbessert werden können.

Umfang der Automatisierung

Wenn Zeit ein so kostbares Gut ist wie im Bereich der Sicherheit, ist die Automatisierung die Rettung. Die Automatisierung der Benutzerschnittstelle (UI) ist, sobald die Anwendung stark und stabil ist, entscheidend für ein schnelles Testen. Ein Shift Right-Ansatz bietet genau diese Plattform.

Breitere Abdeckung

Für eine bessere Qualität und Anwendungserfahrung müssen die Testteams mehr, öfter und so spät wie möglich testen. Ein Shift Right-Ansatz bietet eine viel breitere Testabdeckung mit Zugriff auf das komplette System, da dies in der Postproduktion geschieht. Vergleichen Sie dies mit dem Shift-Links-Ansatz, der in den Planungsphasen zum Tragen kommt, in denen es auf Zeit ankommt und Termine eingehalten werden müssen.

Welchen Weg soll ich gehen?

Im Zuge der Digitalisierung von Unternehmen haben sich verschiedene Testansätze entwickelt. Daher gibt es einen Grund, an beiden Enden des SDLC-Spektrums aktiv zu werden. Mehr Tests, früheres Testen und breiteres Testen tragen alle dazu bei, ein brillantes Produkt zu entwickeln und damit den Aufstieg von SecDevOps als Praxis bei der Bereitstellung sicherer, stabiler und performanter Anwendungen zu unterstützen.

Auch in der digitalen Welt muss jedes Unternehmen, das diesen Namen verdient, sich um den Eindruck kümmern, den es bei seinen Kunden und Mitarbeitern hinterlässt. Und gerade jetzt, inmitten einer globalen Pandemie, könnte aus Sicht des Unternehmens nichts lebenswichtiger sein. Das Testen gleich zu Beginn des Anwendungs-Lebenszyklus und die anschließende Verfeinerung der Testfälle anhand des Benutzerfeedbacks in der Postproduktion sind für Unternehmen unerlässlich, um jede Form der digitalen Glaubwürdigkeit zu gewährleisten.