EBOOK

5 Razones para Priorizar **la Seguridad del Software**

Checkmarx

Introducción

En estos días, la tecnología está evolucionando a un ritmo nunca antes visto, lo que obliga a las organizaciones a una situación de “adaptarse o morir”. A medida que se acelera la transformación digital, todos están sintiendo los efectos. Líderes de DevOps, gerentes de AppSec, y los desarrolladores ciertamente no son una excepción, ya que tienen la tarea de desarrollar e implementar software a un ritmo más rápido para mantener la competitividad y relevancia de sus organizaciones.

Sin embargo, este creciente enfoque en la velocidad a menudo hace que la seguridad se quede en el camino. Simplemente enciende las noticias y probaremos nuestro punto, ya que casi está garantizado que te enterarás de que otra empresa es víctima de un ciberataque. Lo que es especialmente interesante de esto es que la causa principal del problema suele ser el software vulnerable. De hecho, según Forrester, las aplicaciones son el principal vector de ataque para las brechas de seguridad y 42% de los tomadores de decisiones de seguridad global cuyas empresas experimentaron un ataque externo dicen que fue el resultado de una vulnerabilidad de software explotada.

A medida que la proliferación de software continúa, trayendo consigo una superficie de ataque en constante expansión lista para ser atacada por actores maliciosos, proteger el software debe ser una prioridad por encima de todo.

Es hora de cambiar las mareas. Es hora de convertir la complacencia en proactividad. A continuación, presentamos cinco razones por las que es hora de hacer que el software y la seguridad sean inseparables.

#1

El software está en todos lados y se hace más complejo.

El mundo conectado de hoy significa que el software está omnipresente. Simplemente mira a tu alrededor dondequiera que estés leyendo nuestra guía y cuenta la cantidad de cosas que funcionan con software. ¡No olvides incluir el dispositivo que estás utilizando para leer esto!

Desde plataformas de comercio electrónico hasta teléfonos móviles y vehículos modernos, todo está impulsado por billones de líneas de código que han sido escritas meticulosamente por millones de desarrolladores repartidos por todo el mundo. Si bien el software claramente ha permitido a nuestra sociedad hacer más de lo que jamás se había imaginado, no ha estado exento de desafíos, particularmente en lo que respecta a la creación de un inmenso riesgo de seguridad.

A medida que el software se vuelve más omnipresente, adquiere nuevas formas y casos de uso, incorporando una combinación de componentes internos y de terceros, interfaces de programación de aplicaciones (API), nuevas arquitecturas y marcos, contenedores y más. Todo esto conduce a aplicaciones más complejas, que a su vez conducen a aplicaciones más vulnerables y una superficie de ataque ampliada que requiere un mayor énfasis en la seguridad.

El software es el eslabón más débil de toda organización.

Todos hemos escuchado el dicho, “tus mayores activos pueden convertirse fácilmente en tus mayores debilidades “. Bueno, eso se aplica de todo corazón cuando se trata de software. Por un lado, el software es el mayor catalizador de la innovación tecnológica de nuestro tiempo. Por otro lado, con todos los beneficios viene una superficie de ataque masivo que, como industria, no se ha abordado de manera efectiva, lo que ha abierto la puerta a un aluvión de actividad cibernética maliciosa.

El software debe estar protegido. Eso no solo significa proteger las aplicaciones que consideras críticas para tu misión o tu negocio. Una estrategia de seguridad integral involucra toda tu “cartera” de aplicaciones. Aprovechar las soluciones que abordan todas las aplicaciones, ya sean creadas internamente, subcontratadas o mediante componentes de código abierto, y todo el ciclo de vida del desarrollo de software (SDLC) es clave para mejorar tu perspectiva de seguridad.

Las aplicaciones son el principal vector de ataque. 42% de las firmas que experimentaron un ataque afirman que fue resultado de software vulnerable.

Fuente: Forrester Research

#3

Los desarrolladores pueden, y deben, ser una extensión de tu equipo de seguridad.

A medida que la transformación digital se acelera y los equipos de TI se reducen, los desarrolladores han tomado la responsabilidad de entregar software más rápido y al mismo tiempo convertirse en los “guardianes” de la seguridad. Un equilibrio que puede ser complicado de lograr.

La realidad es que la seguridad debería pasar a manos de los desarrolladores. Al final del día, el software vulnerable proviene de errores de codificación que se derivan de descuidos de los desarrolladores. Sin embargo, las expectativas de las organizaciones de que los desarrolladores sean expertos en seguridad de origen es donde las cosas no se alinean del todo.

Los desarrolladores son adaptables por naturaleza y generalmente aceptan el desafío de la seguridad, pero necesitan apoyo a cambio. Las organizaciones deben adoptar soluciones que empoderen y optimicen los flujos de trabajo de los desarrolladores e incorporen la seguridad en cada paso del SDLC para ayudarlos a mantener el ritmo acelerado de los entornos DevOps. Al integrar soluciones automatizadas de pruebas de seguridad de aplicaciones (AST) que se adaptan a la perfección en las canalizaciones de CI/CD, proporcionan retroalimentación de vulnerabilidad en el tiempo con tasas bajas de falsos positivos, menos tareas tediosas y con un retorno de la inversión medible.

Además, para escribir realmente un código más seguro, los desarrolladores deben aprender de los errores del pasado. Con solo el 11% de las organizaciones diciendo que han abordado adecuadamente la necesidad de educación para desarrolladores, se debe poner un mayor énfasis en la implementación de programas dedicados de capacitación y concientización de AppSec. Esta es la forma más eficaz de capacitar a los programadores para que piensen y actúen de forma más segura en su trabajo diario.

Checklist de soluciones DevSecOps

- Automatiza las pruebas de seguridad
- Reduce falsos-positivos
- Elimina tareas tediosas
- Provee ROI medible
- Difunde conciencia y entrenamiento AppSec

El código abierto es tan vulnerable como es valioso.

A medida que los desarrolladores avanzan más rápido, se basan más en el código fuente abierto que en la creación de software desde cero. Las aplicaciones actuales se componen principalmente de bibliotecas y componentes de código abierto y los analistas han descubierto que ahora constituyen el 80-90% del código base promedio. Al final del día, el código abierto es esencial para la innovación. Sin él, muchos de los logros tecnológicos actuales, desde la computación en la nube hasta los dispositivos móviles, no existirían.

Dicho esto, a medida que nuestra industria continúa por lo que parece ser un camino de código abierto primero, también debemos abordar el tema de la seguridad para garantizar que se utilice de manera prudente. Una investigación reciente de RiskSense encontró que el número total de vulnerabilidades en el software de código abierto aumentó en un 130% de 2018 a 2019 (412 a 968 CVE documentados).

Las organizaciones que utilizan software de código abierto, que, seamos honestos, son todas, requieren soluciones que detecten e identifiquen componentes de código abierto o de terceros dentro de sus aplicaciones y proporcionen métricas de riesgo detalladas sobre vulnerabilidades, posibles conflictos de licencias y bibliotecas desactualizadas. Estas soluciones deben integrarse a la perfección en las canalizaciones de CI/CD y SDLC, lo que permite a los equipos de desarrollo, seguridad y DevOps priorizar y centrar los esfuerzos de remediación donde serán más efectivos y eficientes tanto perspectivas de costo y tiempo.

#5

La seguridad del software está en el corazón de la Transformación Digital

Planear cualquier esfuerzo de transformación digital requiere una evaluación de seguridad exhaustiva, especialmente cuando se trata de software. Es fundamental que los líderes organizacionales sean estratégicos en su enfoque de la transformación digital, enfatizando la proactividad en lugar de la reactividad y construyendo la seguridad en los procesos y equipos de desarrollo de software desde el principio.

Seguir un camino de transformación digital no debe hacerse solo y se debe integrar la seguridad del software en cada paso del camino. Ya sea que se implementen nuevas soluciones para permitir que los empleados y desarrolladores trabajen y codifiquen de manera remota, o que se desarrollen la arquitectura y los procesos internos para mejorar la experiencia del cliente, la seguridad es fundamental, ya que un paso en falso podría derribar todo el marco que tanto ha trabajado para construir.

Si la seguridad del software no ha sido una prioridad antes, debe serlo ahora. Es imperativo realizar pruebas de seguridad tempranas en el desarrollo de software, aprovechar las soluciones automatizadas para optimizar los flujos de trabajo y acelerar la corrección de vulnerabilidades, y salvaguardar tu SDLC. A medida que nuestros clientes transforman la forma en que crean e implementan software, Checkmarx se dedica a combinar métodos probados y verdaderos junto con estrategias nuevas e innovadoras para potenciar estos esfuerzos para acelerar el desarrollo de software seguro.

¿Listo para construir más software seguro a la velocidad de DevOps?
¡Contacta a Checkmarx hoy mismo y solicita un demo!

Acerca de Checkmarx

Checkmarx es el líder mundial en soluciones de seguridad de software para el desarrollo de software empresarial moderno. Checkmarx ofrece la plataforma de seguridad de software más completa de la industria que se unifica con DevOps y proporciona una aplicación estática e interactiva para pruebas de seguridad, análisis de composición de software y programas de capacitación y concientización de AppSec para desarrolladores para reducir y remediar el riesgo de las vulnerabilidades del software. Checkmarx cuenta con la confianza de más de 40 de las 100 empresas de Fortune y la mitad de las de Fortune 50, incluidas organizaciones líderes como SAP, Samsung y Salesforce.com. Obtén más información en checkmarx.com.