ZIMPERIUM®
ADVANCED MOBILE SECURITY

Comment le blindage des applications s'intègre dans le cadre de l'approche DevSecOps

Qu'est-ce que le DevSecOps ?

Le cadre DevSecOps intègre la sécurité dans le cycle DevOps standard pour le développement d'applications et de programmes. Il s'agit d'une approche plus traditionnelle du développement qui positionne la sécurité en tant qu'une entité discrète dont le but est de protéger l'ensemble des systèmes d'une organisation, dans le cadre de laquelle les tests de sécurité des applications représentent une fonction parmi d'autres. DevSecOps adopte une approche de test vers la gauche « shift left », selon laquelle les tests sont effectués plus tôt dans le cycle de vie du développement logiciel (SDLC ou Software Development Life Cycle).

Dans un cadre DevSecOps, les meilleures pratiques de sécurité sont intégrées à chaque phase du développement. De cette manière, les applications sont plus sécurisées, présentent moins de vulnérabilités et nécessitent moins de correctifs. Plus précisément, un cadre Agile DevSecOps priorise le maintien de la vitesse de développement sans encourir de dette de sécurité qui devra éventuellement être remboursée par l'organisation.

L'importance du DevSecOps

L'importance de la rapidité de mise sur le marché dans le monde du logiciel préoccupe les équipes de développement. La pression exercée pour suivre l'évolution de la demande, améliorer continuellement les fonctionnalités, tout en livrant rapidement les applications, pousse souvent les équipes à mettre au second plan les questions relatives à la sécurité et aux tests. Une étude faisant le point sur la sécurité des applications mobiles a révélé que 83 % des applications mises sur le marché présentent au moins une faille de sécurité.

Cette pression permanente pousse certaines équipes de développement à adopter une attitude du genre « ship now, patch later » (livrer maintenant, corriger plus tard). Toutefois, comme la plupart des équipes savent, une fois un projet est achevé, on passe directement au suivant, le temps et les ressources alloués à la résolution ¬des problèmes le jour de la sortie ne se concrétisent jamais.

De nouveaux problèmes s'ajoutent à ces failles de sécurité initiales, ils surgissent toujours lorsque des failles sont détectées au niveau du code sous-jacent, des composants tiers ou des bibliothèques de sécurité. Cela provoque une véritable tempête de faiblesses en matière de sécurité et un mauvais suivi des applications, augmentant ainsi le risque de violation des données, de perte de confiance des utilisateurs et de réprimande réglementaire.

Les avantages d'un cadre DevSecOps

Dans un environnement en constant développement, adopter une approche DevSecops reste le meilleur choix pour plusieurs raisons :

1. **Accélérer le temps de développement**
   Les problèmes de sécurité découverts après la phase de développement risquent d'entraîner des retards importants. Intégrer des processus et des tests de sécurité le long du cycle de développement - depuis la planification initiale et jusqu'à la mise en service - limite autant que possible l'obligation de recourir à des -correctifs longs et coûteux par la suite. Cette approche élimine les goulots d'étranglement entre les développeurs et les équipes de sécurité, et qui surviennent souvent dans les environnements non DevSecOps.
2. **Réduire les coûts**
   Publier une application non sécurisée et présentant de nombreuses failles engendre une dette de sécurité qui prend vite de l'ampleur à mesure que le nombre de téléchargements et l'importance structurelle de l'application évoluent. Cette dette coûtera nettement plus cher à rembourser plus tard en matière de risque créé et de coûts potentiels de violations de données, de baisse de productivité et de lourdes amendes pour infraction aux réglementations. L'intégration de la sécurité dès le début grâce à un cadre DevSecOps nécessiterait un coût d'investissement initial plus important, mais elle permettra éventuellement d'économiser d'importants coûts de post¬production en produisant des applications moins sujettes aux failles de sécurité et conformes aux exigences de conformité.
3. **Améliorer l'expérience et la confiance des clients**
   Les utilisateurs finaux peuvent avoir une relation assez compliquée avec la sécurité des applications ; ils veulent que leurs données soient protégées mais n'apprécient pas les mesures onéreuses qui nuisent à leur expérience. Toutefois, les études montrent qu'éventuellement, une sécurité médiocre éloignera les utilisateurs de votre organisation. PwC a constaté que 85 % des utilisateurs éviteront de faire des affaires avec une organisation s'ils ont des préoccupations concernant ses pratiques en matière de cybersécurité et de protection de la vie privée. Un cadre DevSecOps intègre la sécurité et détecte et corrige les problèmes à chaque étape, ce qui donne l'occasion de traiter les éventuelles conséquences sur l'ergonomie.

4. **Des correctifs de sécurité plus rapides**
   Adopter une approche DevSecOps signifie intégrer l'analyse des vulnérabilités et l'application de correctifs en tant que processus dans le SDLC intégré à la gestion du cycle de vie d'une application. Cela permet un support plus sûr et plus rapide après la mise en ligne d'une application, car les membres de l'équipe restent ensemble pour itérer pendant la phase de post-mise en ligne, au lieu d'être distribués et déplacés vers différents projets. En fin de compte, les normes de connaissance et de documentation d'un cadre DevSecOps permettent aux équipes de localiser et de corriger les failles plus rapidement.

Comment le blindage des applications s'intègre dans un cadre DevSecOps

Le blindage des applications joue un rôle majeur dans les efforts déployés par une équipe DevSecOps pour améliorer la sécurité des applications sans compromettre la vitesse de développement ni augmenter les coûts. Allouer un nombre suffisant d'experts en sécurité pour répondre à la demande en matière de développement peut s'avérer difficile ; GitHub estime que le ratio développeur/professionnel de sécurité est de 500:1. Dans le but de suivre le rythme des exigences de sécurité d'un cadre DevSecOps, les équipes en interne ont besoin d'outils faciles à intégrer et qui ne retarderont pas le processus de développement.

Le blindage des applications permet aux équipes DevSecOps de travailler de façon plus efficace en mettant en place un ensemble de protections pour sécuriser le code source et des adresses IP contre les tentatives de rétro-ingénierie et de falsification :

- Falsification du code
- Injection de logiciels malveillants
- Extraction de clés de chiffrement
- Rétro-ingénierie
- Attaques par canal auxiliaire
- Vol de données

L'intégration d'une bonne solution de protection des applications dans le processus de construction permet aux équipes de sécurité de mieux hiérarchiser et gérer les vulnérabilités localisées pendant les tests. Elles peuvent ainsi axer leurs efforts sur la résolution des problèmes critiques, tout en ayant l'assurance de savoir que leur logiciel est capable de résister aux attaques contre les vulnérabilités non corrigées.

Elle offre également une protection contre les éventuelles vulnérabilités qui n'ont pas encore été localisées. Aucune solution de test de sécurité n'est capable de détecter tous les bogues de sécurité et les pirates ne cessent de développer de nouveaux exploits. Une solution de protection in-app efficace permet de sécuriser les logiciels contre ces cas extrêmes et les menaces inconnues.

La suite de protection des applications mobiles de Zimperium s'intègre dans un cadre DevSecOps grâce à une approche multidimensionnelle qui a pour objectif d'immuniser les logiciels contre les attaques. Ceci inclut :

- Obfuscation avancée du code pour lutter contre les tentatives de rétro-ingénierie
- Détection de l'enracinement/de l'effraction, mécanismes anti-débogage et autres protections ayant pour objectif d'empêcher l'analyse statique et dynamique
- Cryptographie en boîte blanche pour protéger les clés de chiffrement contre les tentatives d'exfiltration
- Contrôleurs d'intégrité pour détecter les tentatives de manipulation du code

Conclusion

Ajouter une protection des applications à votre cadre DevSecOps aide à améliorer vos capacités en matière de sécurité sans pour autant surcharger vos outils de sécurité. Cela permet d'atténuer les risques et de répondre aux exigences de conformité en intégrant la sécurité dans les premières phases de votre processus de développement.
Pour plus d'informations sur la manière dont notre protection des applications peut aider vos équipes DevSecOps, prière de nous contacter pour communiquer avec l'un de nos experts en sécurité.

ZIMPERIUM.

4055 Valley View Dallas, TX 75244
844.601.6760
info@zimperium.com