УДК 004.056

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ IT – ПРОЕКТІВ З ВИКОРИСТАННЯМ МЕТОДИКИ DEVSECOPS

Смик Д., Ящук В.
Львівський державний університет безпеки життєдіяльності, Львів

Розглянуто методологію систематизації існуючих засобів захисту програмного забезпечення, що забезпечують взаємодію команди розробників та фахівців із захисту інформації в межах одного життєвого циклу розробки. Проведено класифікаціюпідходів до побудови процесів DevSecOps, проаналізовано необхідні складники для побудови DevSecOps процесів. Проведений аналіз дозволяє класифікувати процес розробленнята захисту програмного забезпечення за допомогою методології DevSecOps.

Ключові слова: *IT – проект, інформаційна безпека, DevOps, DevSecOps.*

The methodology of systematization of the existing means of protection of the software providing interaction of a team of developers and experts on protection of the information within one life cycle of development is considered. The classification of approaches to building DevSecOps processes is carried out, the necessary components for building DevSecOps processes are analyzed. The analysis allows us to classify the process of software development and protection using the DevSecOps methodology.Key words: IT project, information security, DevOps, DevSecOps.

Методологія розробленнята захисту програмного забезпечення в межах DevSecOps змінила підхід до забезпечення безпеки з реактивного на проактивний, а також підкреслює важливість забезпечення безпеки на всіх рівнях організації. DevSecOps означає забезпечення безпеки в розробленні додатків від ранніх етапів до самого завершення, а також включає в себе автоматизацію деяких шлюзів безпеки, щоб запобігти уповільненню робочого процесу DevOps. Необхідно підтримувати короткі і часто повторювані цикли розробки програмного продукту, а також інтегрувати заходи безпеки. Вибір правильних інструментів для безперервної інтеграції безпеки може допомогти в досягненні цих цілей.

Сучасні інструменти автоматизації допомогли підприємствам впровадити більш гнучкі методи розробки, а також відіграли важливу роль у розробленні нових заходів безпеки. Для ефективного захисту DevOps потрібні не тільки нові інструменти, а й зміни на підприємстві процесів DevOps, дляпришвидшення інтегрування роботи груп фахівців з безпеки з іншими спеціалістами, що призведе до покращення якості продукту.

DevSecOps – одна з найважливіших тенденцій DevOps. Це підхід до безпеки операцій, що дозволяє використовувати принципи і кращі практики DevOps для забезпечення кращої, швидкості більш безпечної доставки програмного забезпечення. По суті, це означає, що всі вимоги безпеки з самого початку кодифіковані, а контроль безпеки і розробка здійснюються паралельно, причому безпеку намагаються впровадити в кожну частину процесу agile-розробки. Завдяки цьому DevSecOps може знизити витрати пов'язані з виправленням недоліків безпеки [1].

DevSecOps – це вбудована безпека, а не безпека, яка функціонує як периметр навколо програм та даних. Якщо безпека залишається в кінці конвеєра розробки, організації, що застосовують DevOps, можуть повернутися до довгих циклів розробки, яких вони намагалися уникати в першу чергу.

Зазвичай, методики для оптимізації процесів розроблення програмного забезпечення націлені виключно на підвищення ефективності всередині команди, але в DevSecOps мова йде про застосування автоматизованих інструментів для гарантування комплексного захисту. Варто зазначити, що кожна з доступних методик стрімко прискорює роботу, жертвуючи при цьому безпекою інфраструктури. Більшість компаній може бути не готова до такого стрибка підвищення вимог якості в даній сфері. Саме тому, подальший розвиток DevOps порушив питання інформаційної безпеки. Прискорення роботи команд-розробників створило безперервний потік оновлюваних функцій, а також постійний потік даних з боку сервісів, користувачів та інших додатків [2]. Розгортання коду має відбуватися частіше і завершуватися за менший час. Коротший час циклу є ознакою оптимізованих процесів, в той час як більш тривалий час може бути ознакою того, що необхідно переглянути свої кращі практики або інструменти кодування.

Стратегією DevSecOps є визначення толерантності до ризиків та проведення аналізу ризику. Автоматизація повторюваних завдань є ключовим чинником DevSecOps, оскільки запуск ручних перевірок безпеки в конвеєрі може вимагати багато часу.

DevSecOps дозволяє організації застосовувати попереджуючий підхід до безпеки. Це спонукає розробників програмного забезпечення інтегрувати безпеку в свої повсякденні зусилля. У той же час групи безпеки можуть працювати з розробниками програмного забезпечення, щоб допомогти організації виявити і усунути вразливості безпеки, перш ніж вони вийдуть з-під контролю. DevSecOps змінює безпеку з реактивної на проактивну, а також підкреслює важливість безпеки на всіх рівнях організації, і уповноважує співробітників служби безпеки приймати рішення, які мають позитивний вплив на їхній бізнес.

Таким чином, DevSecOps, як концепція і практика, весь час розвивається, зі збільшенням кількості організацій, які впроваджують DevSecOps як рішення для їх проблеми безпеки [1]. Попит на DevSecOps збільшиться в організаціях всіх розмірів і у всіх галузях. У міру того, як все більше організацій шукають способи виявлення та виправлення проблем безпеки на ранніх етапах процесу розробки програмного забезпечення, попит на інструменти для підтримки DevSecOps відповідно збільшуватиметься.

Підприємство, яке впроваджує інструменти DevSecOps отримує стійку конкурентну перевагу. Надаючи розробникам програмного забезпечення і командам безпеки зручні та ефективні інструменти DevSecOps, підприємство розвиває культуру співпраці, спілкування, прозорості та відкритості. В результаті організація створює середовище, в якій розробники та групи безпеки постійно удосконалюються.

Переваги, які DevSecOps приносить компаніям це – зниження витрат, збільшення швидкості доставки, швидкості відновлення, відповідність в масштабі і пошуку загроз. Сукупний ефект цих переваг – це підвищення ділової репутації та більш плавна бізнес-модель. DevSecOps успішно видалить бар'єри між DevOpsi Security, яка заважають їм працювати як єдине ціле. DevSecOps матиме можливість знаходити і виправляти проблеми безпеки на початку процесу розробки, тим самим значно скорочуючи витрати, пов'язані з їх виявленням і виправленням. Важливо включити гарантування безпеки в життєвий цикл розробки Agile. Завдяки DevSecOps розробники можуть краще зрозуміти критичність уразливостей, які існують у їхньому коді, і виправити ці вразливості, надаючи швидкі, але безпечніші продукти або рішення. Оскільки підхід DevSecOps автоматизований, тому команді розробників більше не потрібно записувати правила безпеки у свій код. DevSecOps знижує ризик перенапруження даних, оптимально застосовуючи ресурси.

Література

1. IT - безпека [Електронний ресурс] Режим доступу до ресурсу: https://astwellsoft.com/uk/blog/software-security.html.

2. Чим займається DevOps – інженер [Електронний ресурс] // Режим доступу до ресурсу: https://vc.ru/hr/51144-kto-takoy-devops-inzhener-i-chem-on-zanimaetsya.

3. Що таке DevSecOps [Електронний ресурс] // Режим доступу до ресурсу: https://itfb.com.ua/chto-takoe-devsecops/.

4. Ящук В. І. Тренди використання технології «хмарних обчислень» в ІТ-сфері України / В. І. Ящук // Торгівля, комерція, підприємництво : збірник наукових праць / [редакц. кол.: Апопій В. В., Дайновський Ю. А., Скибінський С. В. тощо.]. – Львів : Львівська комерційна академія, 2012. – Вип. 14. – С. 104-108.