DIGITALNO INOVACIJSKO STIČIŠČE SLOVENIJE
REPUBLIKA SLOVENIJA MINISTRSTVO ZA GOSPODARSKI RAZVOJ IN TEHNOLOGIJO
EVROPSKA UNIJA EVROPSKI SKLAD ZA REGIONALNI RAZVOJ NALOŽBA V VAŠO PRIHODNOST
I FEEL SLOVENIA
Naložbo sofinancirata Republika Slovenija in Evropska unija iz Evropskega sklada za regionalni razvoj.

Razvoj in kibernetska varnost

Gregor Spagnolo, SSRD d. o. o.

Povzetek — Največjo kibernetsko grožnjo za podjetja, ki se ukvarjajo z razvojem programske opreme, predstavlja skromno namenjanje pozornosti varnemu razvoju programov in/ali spletnih aplikacij. Podjetja ogromno časa in energije posvetijo končnemu izgledu produkta, pri tem pa pozabljajo na pomen kibernetske varnosti v času razvoja ter načrtovanja aplikaciji in sistemov. Neposvečanje pozornosti kibernetski varnosti ne izhaja samo z razvijalskega stališča, ampak tudi z nezadostnega poznavanja problemov in tveganj, ki jih je potrebno upoštevati pri razvoju. Zato je izobraževanje razvijalcev tudi na področju kibernetske varnosti ključnega pomena za razvoj produkta, ki lahko parira v svetovnem merilu.

Ključne besede — kibernetska tveganja, OWASP Top 10, razvoj aplikacij, SecureBank

Abstract — The biggest cyber threat for software development companies is the lack of attention to the secure development of programs and/or web applications. Companies dedicate a huge amount of time and energy to the final look of a product while forgetting the importance of cybersecurity during the development and design of applications and systems. The lack of attention to cybersecurity stems not only from a developer's point of view but also from a lack of knowledge of the problems and risks that need to be considered in the development. Therefore, educating developers in the field of cybersecurity is also crucial for the development of a product that can compete on a global scale.

Keywords — Cyber risks, OWASP Top 10, web application, SecureBank

1. UVOD

Kibernetska varnost predstavlja zapleteno vprašanje za podjetja, ki se ukvarjajo z razvojem programske opreme. Vsako podjetje, s svojimi storitvami in izdelki, ima namreč svoje posebnosti ter zahteve, zaradi katerih so rešitve prilagojene vsakemu primeru posebej. Zavoljo tega so trenutne varnostne rešitve zapletene in zahtevajo posebno strokovno ekipo, posledično pa predstavljajo velik zalogaj, tako s finančnega kakor tudi s časovnega vidika. V nadaljevanju bo predstavljen slovenski projekt SecureBank. Na projektu lahko pridobite podrobnejše informacije in se na praktičnih primerih seznanite z vsemi OWASP top 10 ranljivostmi.

2. PREGLED PODROČJA

Razvijalci programske opreme se dandanes ne soočajo zgolj z izzivi, ki jih prinaša programiranje, temveč tudi z novimi varnostnimi izzivi. Zato niso le strokovnjaki za kodo, ampak so nekoliko prisiljeni poznati tudi osnove varnosti informacijskih sistemov. Kljub njihovim obsežnim prizadevanjem za odpravo običajnih ranljivosti te še vedno lahko najdemo v aplikacijah in so pogosto posledica neustreznega programiranja ali neupoštevanja dobrih praks varnega razvoja.

Dober primer prakse varnega razvoja je postavilo podjetje Microsoft, ki je kot prvo začelo s spremembami lastnega procesa razvoja in vzdrževanja programske kode. Podjetje je prešlo iz običajnega kroga razvoja (angl. DLC Development Lifecycle) ter dodalo nov pomemben parameter razvoja (tj. kibernetsko varnost) in preimenovalo razvojni proces v SDLC (Security Development Lifecycle).

Čeprav se lahko zdi preprečevanje dostopa kibernetskim kriminalcem do sredstev in podatkov kot zastrašujoča naloga, obstaja nekaj preprostih ukrepov, ki jih lahko podjetja uporabijo za upravljanje kibernetskih tveganj in omejevanje izpostavljenosti.

FinTech aplikacijski projekt SecureBank prikazuje, kako razvijalci pogosto ne uspejo zaščititi svojega okolja zaradi pomanjkanja znanja o uporabljenem ekosistemu. Projekt razvijalcem omogoča določitev Pomaga dockerjeve uporabe mikroservisnih rešitev in kje razvijalci pogosto napačno konfigurirajo sisteme. V aplikaciji so tudi predstavljene in na praktičnih primerih prikazane ranljivosti iz seznama OWASP Top 10.

Z aplikacijo SecureBank se razvijalci seznanijo z najbolj pogostimi tveganji, ki jih pogosto pozabijo in so del OWASP Top 10. Aplikacija ponuja ozaveščanje in usposabljanje, orodja za opredelitev, odkrivanje in reševanje ranljivosti, orodja za zaščito in odzivanje na nevarnosti ter varnostna priporočila. Tako lahko povsem sami najdejo ranljivosti ter jih rešijo s preprostimi orodji in lekcijami, dostopnimi v

aplikaciji. Podjetjem pomaga razumeti varnostna tveganja, ki bi jih morali upoštevati in vzeti v obzir. Zlasti mikro, mala in srednje velika podjetja, ki se ukvarjajo z razvojem programske opreme, imajo pogosto malo strokovnjakov za informacijsko varnost.

Izvorno kodo SecureBank lahko preverite na GitHubu ali jo naložite iz DockerHub-a.

LITERATURA

[1] Microsoft. What are the Microsoft SDL practices?. Dostopno na spletnem naslovu: https://www.microsoft.com/en-us/securityengineering/sdl/practices

[2] SecureBank. Docker hub. Dostopno na: https://hub.docker.com/r/ssrd/securebank

[3] SecureBank. Gitbook. Dostopno na: https://ssrd.gitbook.io/securebank/

[4] SecureBank. Github. Dostopno na: https://github.com/ssrdio/SecureBank