Analýza a plánovanie rizík v softvérovom projekte

HOANG XUAN LINH

Slovenská technická univerzita
Fakulta informatiky a informačných technológii
Ilkovičova 3, 842 16 Bratislava
linh@ynet.sk

Abstract. Ministerstvo obrany US (DoD) pripustí, že manažment rizík je nevyhnutný proces úspešného projektu [2]. Cieľom manažmentu rizík je minimalizovať možnosť zhmotnenia rizika alebo minimalizovať účinok jeho skutočného zhmotnenia. Táto esej nepredstavuje celý proces manažmentu rizík, ale dáva ucelený pohľad dvoch dôležitých jeho fáz, t.j. fáza analýzy a plánovania. Analýza je druhá a najdôležitejšia fáza manažmentu rizík s cieľom odpovedať na otázku „Aké veľké je riziko?“. Nielen analyzujeme riziká a ich efekty, ale aj faktory, ktoré môžu byť dôvodmi rizika. Pokiaľ plánovanie je nasledujúca fáza analýzy s cieľom odpovedať na otázku „Čo je perspektíva projektu na adresovanie toho nepriateľského následku?“. Cieľ tejto eseje umožňuje čitateľovi efektívne riadiť riziká počas fáz analýzy a plánovanie rizík projektu. Esej tiež poskytuje prehľad a klasifikáciu bežných rizikových faktorov identifikovaných skúsenými projektovými manažérmi.

Úvod

Študenti alebo tiež neskúšaní programátori majú často nedokončené alebo neúspešné projekty. Jeden z hlavných dôvodov je nedostatočný manažment rizík. Ľudia sa len snažia produkovať nejaké výstupy a si často zabudnú na potenciálne riziká v ich projekte. Keď projekt zlyhá tak nie len stratia čas na úpravu chýb ale aj stratia dôveru partnerov, klientov, atď. Podľa [4] v roku 1995 firmy v Spojených Štátoch musia zaplatiť výdavky okolo 81 miliárd dolárov pre zrušenie softvérového projektov. Tak manažment rizík sa treba brať do úvahy pri vývoji softvérového projektu.

Analýza rizík je jedna fáza manažmentu rizík, ale často pojem analýza a manažment rizík sú susedné vo viacerých literatúrach, z toho vyplýva, že analýza je jadro manažmentu rizík. Nemôžeme diskutovať o manažmente rizík bez analýzy rizík. A naopak, keď hovoríme o analýze rizík tak ide nám aj o manažment rizík. Výstup fázy analýzy je pre spracovanie fázy plánovania. Budeme podrobne rozobrať tie fázy v článku 3, 4.

Manažment v softvérovom inžinierstve, október 2006, s. 1-8.

Riziko a manažment rizík

Existuje veľa verzií definície pre riziko, ale podľa [1] tak riziko je možnosť utrpieť stratu, poškodenie, nevýhodu alebo zničenie. Riziko môže byť spojené so všetkým aspektmi projektu. Z pohľadu manažmentu softvérového inžinierstva slovo riziko nemusí vždy mať negatívny dopad ale môže mať aj pozitívny dopad. V tomto dokumente budem používať slovo riziko v jeho častejšie používanom, t.j. negatívom význame.

Manažment rizík v softvérovom projekte pomáha predchádzať nepredvídaným udalostiam, najmä katastrofám a veľkým stratám. Cieľom manažmentu rizík je minimalizovať možnosť zhmotnenia rizika alebo minimalizovať účinok jeho skutočného zhmotnenia [4]. Manažment rizík sa môže rozdeliť na nasledujúce fázy [1]:

- Identifikácia – určenie, aké riziká môžu ohroziť projekt a dokumentovanie ich charakteristík.
- Analýza rizík – vyhodnotenie rizík a určenie, ktoré riziká vyžadujú nejakú akciu, stanovenie priority rizík a analýza možných reakcií na udalosti spôsobujúcej škody.
- Plánovanie rizík – definovanie krokov pri výskyte udalosti spôsobujúcej škody.
- Riadenie rizík – vykonanie plánu manažmentu rizík, sledovanie stavu projektu, zabezpečenie činnosti manažmentu pri zmenách.

Zaujímajú nás v tejto eseji len fázy analýza a plánovanie.

Analýza rizík

Analýza rizík je druhý krok v procese manažmentu rizík. Možné hrozby sú identifikované a mapované na riziko, ktoré je s nimi spojené. Výsledok tejto analýza rizík umožňuje identifikovať vhodné riadenie na zníženie alebo odstránenie rizík v rámci procesu rizikového zmiernenia. Riziko je funkcia pravdepodobnosti danej hrozby použitím možnej zraniteľnosti a výsledný vplyv tejto škodlivej udalosti na informačné prostriedky [3]. Aby sme zistili pravdepodobnosť vzniku škodlivej udalosti, hrozieb v systéme musí byť analyzované v súvislosti s možnými zraniteľnosťami a bezpečnosťami systému.

Spracovanie metodológie rizika smeruje na základné kroky:

1. Ohodnotenie zraniteľnosti v architektúre projektu
2. Analýza hrozby
3. Zistenie pravdepodobnosti rizika
4. Zistenie vplyvu rizika

Ohodnotenie zraniteľnosti v architektúre projektu

Tri činnosti môže zapríčiniť v tejto fáze, to sú:

1. Analýza známej zraniteľnosti
2. Analýza viacznačnej zraniteľnosti.
3. Analýza zraniteľnosti vnútorného platformu.

Analýza známej zraniteľnosti

Existujú rôzne druhy známej zraniteľnosti, ktoré sú dokumentované v literatúre softvérovej bezpečnosti. Rozsah týchto zraniteľností pohybuje od napr. jasné ako (nemôže autentizovať) do jemnej formy ako (manažment symetrického kľúča).

Analýza viacznačnej zraniteľnosti

Je to bohatý zdroj zraniteľností keď existuje medzi požiadavkami alebo špecifikáciami a vývojom. Hlavná úloha toho kroku je odstrániť nejasnosti medzi požiadavkami a implementáciami. Dôležité je dať do úvahy kde požiadavky sú viacznačné napísané a kde implementácia nesúhlasí alebo neúspešne vyrieši. Napr. požiadavka pre webovú aplikáciu môže hlasí, že administrátor môže blokovať konto a tento používateľ už nemôže prihlásiť do systému pokiaľ konto je zablokované. Čo by sa stalo ak používateľ je aktívne prihlásený v systéme a vtedy admin. ho nablokuje? Bude používateľa odhlási alebo jeho sekcia bude ešte platná kým neodhlási? Autentifikácia a autorizácia architektúry musia byť porovnané s aktuálnou implementáciou pre vedenie akým spôsobom boli tieto otázky riešené. Rozvetvenie bezpečnosti pre log-in, ktorý trvá aj mimo blokovania konta musí byť uvažované ako proti citlivosti informačných zdrojov.

Analýza zraniteľnosti vnútorného platformu

Cieľ toho kroku je vytvoriť zoznam aplikácií alebo zraniteľností systému, ktorý vyskytuje náhodne alebo zámerne pokazí a účinkuje poruchu v bezpečnosti alebo poruší etiku systémovej bezpečnosti.

Analýza hrozby

Hrozby sú činitele, ktoré porušia obranu informačných zdrojov a etiku bezpečnosti stránok. Analýza hrozieb identifikuje pre špecifickú architektúru, funkcionalitu a konfiguráciu. Analýza hrozieb môže predpokladať danú úroveň prístupnosti a úroveň zručnosti, ktorú môžu útočníci vlastniť. Hrozby môžu byť mapované do zraniteľností aby pochopili ako systém môže porušený. Plán pre zmiernenie je zložený s opačnými spôsobmi, ktoré sú schopné účinkovať proti identifikovaným zraniteľnostiam porušené hrozbami.

Príklad hrozby sú generovanými individuálne krekermi. Ich zámer je hlavne poškodiť informačné systémy a získať počítačové techniky. Tabuľka 1 syntetizuje potenciálne hrozby pre softvérové projekty podľa [3].

Threat Source	Motivation	Threat Actions
Cracker	Challenge Ego Rebellion	• System profiling • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	• Computer crime (e.g., cyber stalking) • Fraudulent act (e.g., replay, impersonation, interception) • Information bribery • Spoofing • Botnets • Malware: Trojan, virus, worm, spyware • Spam • Phishing
Terrorist	Blackmail Destruction Exploitation Revenge Monetary gain Political gains	• Bomb • Information warfare • System attack (e.g., distributed denial of service) • System penetration System tampering

Tab. 1 Potenciálne hrozby pre softvérové projekty

Zistenie pravdepodobnosti rizika

Po zistení ktoré hrozby sú dôležité a ktoré zraniteľnosti môžu byť prerušené, bude to užitočne odhadnúť pravdepodobnosť rôznych možných rizík. V softvérovej bezpečnosti „pravdepodobnosť“ je kvalitatívny odhad o úspešnom prerušení podľa analýzy a minulej skúseností. Pokiaľ závisí od minulej skúseností, tak táto

pravdepodobnosť nemôže zodpovedať pre nové druhy útokov alebo zraniteľností, ktoré sú ešte nenájdené. To nemusí definitívne odrazí pravdepodobnosť úspešného útoku. Napriek tomu, koncept pravdepodobnosť môže byť užitočný pre stanovenie priorít rizík a ohodnotenie účinnosti o očakávaných zmierneniach.

Musíme dať pozor na nasledujúce ocenenia pravdepodobnosti:

- Zámer hrozieb a ich schopnosť
- Otvorenosť zraniteľností a ich vplyvov
- Účinnosti doterajšieho riadenia

Pravdepodobnosť je subjektívna kombinácia týchto troch uvedených veličín. Tieto veličiny môžeme uviesť ako vyššie, stredné a nízke. Podľa [3] máme tabuľku 2.

High	The three qualities are all weak: a threat is highly motivated and sufficiently capable, a vulnerability exists that is severe and direct, and controls to prevent the vulnerability from being exploited are ineffective
Medium	One of the three qualities is compensating, but the others are not. The threat is perhaps not very motivated or not sufficiently capable, the controls in place may be reasonably strong, or the vulnerability might be indirect or not very severe.
Low	One of the three qualities is compensating, but the others are not. The threat is perhaps not very motivated or not sufficiently capable, the controls in place may be reasonably strong, or the vulnerability might be indirect or not very severe.

Tab. 2 Pravdepodobnosť rizika

Zistenie vplyvu rizika

Zistenie vplyvu rizika obsahuje dve aspekty:

- Identifikovanie ohrozených zdrojov
- Zistenie vplyvu lokality

Identifikovanie ohrozených zdrojov

Ohrozené zdroje vplyvom rizika a typ následku musia byť identifikované. Obyčajné vplyvy v informačných zdrojoch zahrňuje stratu údajov, ich korupciu a neautorizovanú alebo neauditovanú modifikáciu dát, nedostupnosť dát a vloženie neplatných údajov.

Zistenie vplyvu lokality

Každý vplyv má lokalitu v priestore, čase, zásade a v práve. Okrem vplyvu z finančného hľadiska, umiestnenie v iných dimenzií môže byť užitočné alebo požiadané. Napr. ak šifrovací kľúč je uložený ako nešifrovací, zaujíma nás či je to alokovaný dynamicky na RAM-ke aplikácií v serveri alebo na pevnom disku na internete, alebo v pamäti klientskej aplikácie.

Už sme hovorili o pravdepodobnosti vzniku a vplyve rizika, potom získame hodnotu rizika ako súčin vplyvu rizikovej udalosti a pravdepodobnosti, že udalosť nastane. Môžeme ho vyjadriť nasledovaným vzorcom.

$V(A) = P(A) * C(A)$

Kde P(A) je pravdepodobnosť, že nastane udalosť A, C(A) vyjadruje vplyv udalosti A a V(A) je hodnota rizika pre udalosť A. Vidíme, že hodnota rizika je úmerná s pravdepodobnosťou rizika a vplyvom rizika. Ak vplyv je veľký ale pravdepodobnosť je veľmi malá tak môže vyplývať aj hodnota rizika malá. Tak na výpočet hodnoty rizika musíme brať do úvahy obidva faktory. Nemôžeme ohodnotiť nízke hocijaký faktor.

Plánovanie rizík

Plánovanie rizík znamená definovanie krokov pri výskyte udalosti spôsobujúcej škody. Zámer plánovania rizík je odpovedať na otázku „Čo je perspektíva projektu na adresovanie toho nepriateľského následku?“. Často používame pojem plánovanie rizikového zmiernenia za pojem plánovanie rizík. Jedna alebo viac možnosti zmiernenia môže byť:

- Vyhnutie rizika elimináciou hlavnej príčiny a/alebo následkov.
- Riadenie dôvodu alebo následkov
- Transformácia rizika
- Predpovedanie úrovne rizík a pokračovanie v súčasnom pláne projektu

Plánovanie rizikového zmiernenia sú činnosti, ktoré identifikuje hodnoty a vyberie možnosti pre nastavenie rizík na akceptovateľnej úrovni daného projektového obmedzenia a cieľu. Plánovanie rizikového zmiernenia umožňuje dosiahnuť úspech projektu. To zahrňuje čo musí robiť, kedy musí byť urobené, kto je zodpovedaný a fondy, ktoré sú požiadané na jeho implementáciu. Najvýhodnejší projektový prístup sa vyberie z možnosti zmiernenia v uvedených zoznamoch dokumentovaný na plán rizikového zmiernenia.

Úlohy plánovania rizikového zmiernenia

Pre každý hlavný dôvod rizika, typ zmiernenia musí byť zistený a ich detaily musia byť opísaný.

Zmiernenie rizikového plánu je potrebné aby bolo realistické, dosiahnuteľné, merateľné a dokumentované podľa [2] obsahuje nasledujúce hlavičky.

- Opisujúci titul pre identifikované riziko
- Dátum plánu
- Miesto kontraktov zodpovedajúce na riadenie hlavnej identifikovanej príčiny.
- Krátky opis o riziku (vrátane krátky záver o vykonaní, súpise a vplyve zdroja, pravdepodobnosti výskytov, následkov, či je riziko v rámci riadenia programu).
- Prečo existujú tieto riziká (hlavné zapríčiňujúce dôvody).
- Výber zmiernenia (potenciálne možnosti pre odstránenie rizika)
- Definícia udalostí a činností zameraná na zníženie rizika, kritéria úspechu pre každý plán udalosti a nasledujúce „hladina rizík ak je úspešné“ hodnoty.
- Stav rizík (stručne diskutuje)
- Prístup ústupu (opisuje prístupy a očakávame dátum rozhodnutia pre uvažovanie implementácie)
- Odporučenie manažmentu (či rozpočet alebo čas musí byť alokovaný a či alebo nie zmiernenie rizika je zahrnuté v odhade na koniec alebo na inom pláne projektu)
- Úrovne vhodného pristúpenia (každý člen má inú rolu tak má inú úroveň)
- Identifikovanie zdroja potreby.

Treba si uvedomiť, že plánovanie rizikového zmiernenia môže analyzovať hrozby a zraniteľnosti pre projekt. Potom fáza analýza rizík len vyjadruje profil rizikového zmiernenia.

Záver

Analýza a plánovanie rizík sú procesy na rozpoznanie a zmiernenie efekty dopadov neočakávaných udalosti. V fáze analýzy sme uviedli dostatočné aspekty rizika. A potom v fáze plánovania sme sa tiež poskytnúť zámer a úlohy plánu rizikového zmiernenia. Riziko môže ovplyvňovať hocikedy a na všetky aspekty projektu tak treba si uvedomiť, že obránenie vplyvov rizík nie je práca konkrétneho ale všetkých členov projektu a nie je v konkrétnom čase ale v celom živote projektu.

Odkazy na literatúru

1. Bieliková, M: Softvérové inžinierstvo. Princípy a manažment. Vydavateľstvo STU, Bratislava 2000, 141-143
2. Risk management guide for dod acquistion. Six Edition, August 2006, Department of Defense, 1-2
3. Paco Hope, Steven Levenhar, Gunnar Peterson: Architectural Risk Analysis, 2005 Cigital.
4. Mark Keil, Paul E. Cule, Kalle Lyytinen and Roy C. Schmidt: A framework for identifying software project risks. November 1998/Vol. 41, No. II Communications of the ACM, 76
5. Geoffrey Groy: A risk management framework for Software Engineering Practice, 2004 Australian Software Engineering Conference (ASWEC'04).

Annotation

Risk analysis and planning in software project

Department of Defense US (DoD) recognizes that risk management is indispensable process to project success. The objective of risk management is to minimize reification of risk or to minimize impact of risk's real reification. This essay doesn't introduce all processes of risk management but only offers a complex overview of two important phases that is phase risk analysis and planning. Analysis is a second and most important phase of risk management with the intent to answer the question “How big is the risk?” We don't only analysis risks but also analysis their effects or factors that can cause a risk. While planning is following phase of analysis with intent to answer the question “What is the project approach for addressing this potential unfavorable consequence?” Purpose of this essay is to help reader in effectively managing risks during analysis an planning phase. This essay also provides an overview and a classification of usual risk factors identified by experienced project managers.