

KREDĪTU SALĪDZINĀŠANAS PLATFORMAS RISKU ANALĪZE RISK ANALYSIS OF DIGITAL LOAN COMPARISON PLATFORM

Autore: **Jelena ŠČETILNIKOVA**, e-pasts: scetilnikova@inbox.lv
Zinātniskais vadītājs: Dr.sc.ing., doc. **Sergejs KODORS**
Rēzeknes Tehnoloģiju akadēmijas

Abstract. *Advanced technologies can improve the efficiency of business processes, but incorrect system implementation can also become a huge source of damage. Therefore, the issue of IT security is very important. The concept of IT security has many aspects. One of them is security risk analysis, which must be considered by each system developer. The article describes one of the risk analysis methods - the CORAS method. The goal of research was to complete the risk analysis of the loan comparison platform. As a result, the risk mitigation recommendations were developed.*

Keywords: *credit comparison platform, CORAS, risk analysis.*

Ievads

Viedo un informācijas tehnoloģiju ietekme ir būtiskā mūsdienīgas tautsaimniecības izaugsmē. Tehnoloģijas spēj ne tikai uzlabot biznesa procesu efektivitāti, bet arī kļūt par nopietnu postījumu avotu, ja tos pielietot neapdomīgi. Mūsdienās lielākā biznesa procesu un komunikāciju daļa, kā arī daudzas ikdienas aktivitātes, ir saistītas ar IT pielietojumu. Tas ir būtiski izstrādāt sistēmu, netikai ievērojot lietotāju prasības, bet arī drošības aspektus. Drošības jautājumi ir vieni no nozīmīgākajiem mūsdienīgajā IT industrijā. Vīrusi, tārpi, nesankcionēta piekļuve datiem, haķeru uzbrūkumi ir plaši dzirdāmi draudi, kas var salauzt vai apturēt digitālas sistēmas darbību.

IT drošības jēdzienam ir daudz aspektu. Viens no tiem ir drošības riska analīze, kas ir būtiska jebkādas inženiertehniskās sistēmas izstrādes procesā, sistēmas lietotājam vai sistēmas īpašniekam, lai iegūtu kontroli un zināšanas par sistēmas drošības līmeni. IT riski jāpārvalda tāpat kā tradicionālie biznesa riski. IT risku pārvaldība sastāv no to periodiskas novērtēšanas un pasākumu īstenošanas, lai identificētus riskus samazinātu līdz pieņemamam līmenim. Tajā pašā laikā vajag pareizi novērtēt iespējamus riskus un zaudējumus, lai noteiktu saprātīgu ieguldījumu apjomu risku mazināšanai.

Drošības analīzes ir dārgas un laikietilpīgas, to nevar veikt no sākuma katru reizi, kad sistēma tiek atjaunināta vai modificēta, tāpēc ir nepieciešama metodoloģija, kura spēj viegli papildināt esošu analīzi. Kā viens no risinājumiem ir izstrādāta CORAS risku analīzes metode.

Pētījuma mērķis ir izpildīt risku analīzi kredītu salīdzināšanas platformas lietošanas gadījumam. Mērķa sasniegšanai ir izvirzīti šādi uzdevumi: (1.) klasificēt iespējamus IT riskus; (2.) izstrādāt CORAS risku modeli; (3.) izstrādāt rekomendācijas risku samazināšanai.

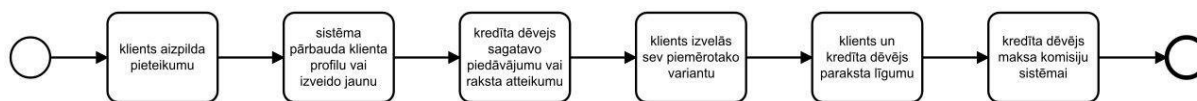
Pielietotās metodes: aprakstošā metode, analīze un klasifikācija, modelēšana, CORAS metode.

Materiāli un metodes

Pirms sākt identificēt un analizēt iespējamus riskus, sākumā jāiepazīstinās ar analīzes sistēmu. Ar citiem vārdiem sākot, mums vajag saprast kas mums jāizsarga, pirms varam saprast kas un kā tam var draudēt vai kaitēt.

Kredītu salīdzināšanas platforma ir informācijas sistēma, pielietojot kuru, varēs sekmīgi sadarboties kredītu dēvēji un kredītuņēmēji, katrs īstenojot savu uzdevumu un lomu. Šajā platformā jebkurš potenciālais kredītaņēmējs var aizpildīt kredīta salīdzināšanas pieteikuma formu, vienu reizi aizpildot nepieciešamo informāciju un pievienojot nepieciešamus dokumentus, un saņemt kredītēšanas piedāvājumus no dažādiem kredīta devējiem, - rezultātā

izvēlēties sev piemērotāko un visizdevīgāko finansēšanas variantu. Šis biznesa process ir attēlots *BPMN2* diagrammā (skat. 1. attēlu):



1. attēls. Īss biznesa procesa apraksts

BPMN ir standartizēta plūsmas diagrammu izveides metode, kas ļauj izveidot un kopīgot viegli saprotamas diagrammas biznesa procesa aprakstīšanai [1].

Šajā sistēmā ir iesaistīti trīs dalībnieki:

- Klients - juridiskā persona, kura vēlas saņemt kredītu;
- Sistēma jeb platformas konsultants – darbinieks vai automatiskie procesi, kuri kontaktē ar klientu un kredīta devējiem;
- Kredīta devējs - partneris, kurš sniedz kredītēšanas pakalpojumus, pielietojot šo sistēmu.

Risku analīze būs veikta, izmantojot *CORAS* metodi. Saskaņā ar metodes vadlīnijām, informācijas sistēmas tiek uzskatītas ne tikai no izmantoto tehnoloģiju viedokļa, bet kompleksā kā sociotehniska sistēma, kurā tiek ņemts vērā arī cilvēciskais faktors. *CORAS* metodoloģija ir izstrādāta Informācijas sabiedrības tehnoloģiju programmu ietvaros. Tās būtība ir tādu riska analīzes metožu kā *Event-Tree-Analysis*, *Markov Chains*, *HazOp* un *FMECA* pielāgošana, pilnveidošana un apvienošana [2]. *CORAS* metodika ir atbalstīta ar rīku, izstrādātu *Java* valodā [3].

Risku analīze saskaņā ar *CORAS* metodi sastāv no septiņiem posmiem [4]:

- 1. posms:** ievadsapulce, kura analītiķi iepazīstinās ar projektējamu vai esošu sistēmu;
- 2. posms:** analītiķi identificē pirmāros draudus un incidentus;
- 3. posms:** mērķis ir precizēt izstrādāto modeli, kuru apstiprina klients;
- 4. posms:** analītiķi papildina, detalizē un precizē nevēlamo incidentu, draudu un ievainojamību sarakstu;
- 5. posms:** seku un to varbūtību novērtēšana katram no identificētajām incidentam;
- 6. posms:** vispārējās analīzes rezultāta prezentācija klientam, ka parasti tam seko uzlabojumi un korekcijas;
- 7. posms:** veltīts uzlabošanai, izmaksu un ieguvumu jautājumu risināšanai.

Rezultāti un diskusija

Risks ir pozitīvs vai negatīvs notikums, kas var izpildas ar noteiktu varbūtību un spēj ietekmēt uz sistēmas darbību un atsaukties uz uzņēmējdarbības vērtībām. Riski ir ārējie un iekšējie faktori vai faktoru kopums, kas var aizkavēt vai mainīt projekta gaitu, vai apdraudēt tas realizācijai. Galvenā risku pazīme ir neparedzamība, tāpēc ir svarīgi sagatavoties reaģēt uz riskiem savlaicīgi vai samazināt to varbūtību. Katrs lietotājs un viņa darba vieta nes savus riskus, bez lietotājiem sistēmai var nest riskus arī darba vides faktori: hakeri, tīkla nepilnības, u.c. [5].

Projekta riski ir identificēti un aprakstīti 1. tabulā, izmantojot *CORAS* metodi [6]:

Projekta riski

Kurš vai ko izraisa risku?	Kā? Kāds ir incidents?	Kas padara to iespējamu?
Hakeris	Ielaužas sistēmā un nozog datus vai ielaiž vīrusu	Nepietiekama drošība
Tehnika	Datoru var salauzt, kļūdas programnodrošinājumā, tīkla problēmas	Nepietiekama aprīkojuma un pakalpojumu kvalitāte
Lietotājs „Klients”	Ielāde inficētu dokumentu	Nepietiekama drošība
Lietotājs „Klients”	Ievada viltotus vai nepatiesus datus	Sistēma nepārbauda datu patiesumu
Lietotājs „Konsultānts”	Bez pamatojuma maina datus pieteikumos	Procedūru neievērošana
Lietotājs „Konsultānts”	Neseko līdz pieteikumu statusam	Procedūru neievērošana
Lietotājs „Konsultānts”	Laicīgi neatbild uz jautājumiem	Procedūru neievērošana
Lietotājs „Konsultants”	Nekvalitatīva klientu konsultācija	Personāla nepietiekoša profesionalitāte
Lietotājs „Konsultānts”	Izmanto datoru savām vajadzībām, kas neattiecas uz darbu	Nepietiekama drošība un procedūru neievērošana
Lietotājs „Konsultānts”	Informācijas izpaušana trešajai personai	Nepietiekama drošība
Lietotājs „Kredīta devējs”	Laicīgi neapstrādā pieteikumus	Procedūru neievērošana
Lietotājs „Kredīta devējs”	Informācijas izpaušana trešajai personai	Nepietiekama drošība

Nākamais solis ir diagrammas sagatavošana, izmantojot *CORAS* rīku [5] (skat. 2. attēlu).

samazināšanas. Vislielāku risku skaitu nes platformas konsultants, viņa neprofesionalitāte var būt nekvalitatīvas konsultācijas iemesls, iekšējo procedūru neievērošanas rezultātā kredīta pieteikums var nebūt laicīgi apstrādāts un klients būs pazaudēts. Gan platformas konsultantam, gan kredīta devējam ir pieejas klientu datiem, sakarā ar to eksistē risks, kas ir saistīts ar datu nodošanu trešai personai, dati var būt izmantoti citiem mērķiem, kas, savukārt, ir nelikumiska rīcība un ved pie finanšu un klientu uzticības zaudējumiem. Tehnika, savukārt, arī nes riskus, jo programmas kļūdas un vīrusi var traucēt normālam darbības ritmam, rezultātā klientu pieteikumi var nebūt laicīgi apstrādāti.

Nākošais solis būs darbību kopuma noteikšana vai izstrāde, kuri var mazināt katra incidenta varbūtību. Piemērām datoru regulāra tehniska apkope var mazināt bojājumu varbūtību līdz pat nulles procentam. Konsultantu regulāra apmācība un testu nokārtošana var paaugstināt klientu konsultācijas kvalitāti.

Secinājumi

Ir uzzīmēta sākotnēja riska analīzes diagramma, bet projekta darbības gaitā tā būs papildināta gan ar jauniem risku incidentiem, gan ar risku mazināšanas pasākumiem. Jo risku analīze ir pastāvīgs un sistematizēts darbs katra projekta ietvaros. *CORAS* metode neļauj novērtēt drošības pasākumu īstenošanā veikto ieguldījumu efektivitāti, neparedz pārvaldības metožu efektivitātes novērtēšanas mehānismus. Bet viena no *CORAS* metodes pozitīvas puses ir tāda, ka programmnodrošinājums, kas realizē šo metodiku, tiek izplatīts bezmaksas un tā instalēšanai un ieviešanai nav nepieciešami ievērojami resursi.

Darba izvirzītie uzdevumi ir izpildīti: projekta riski ir klasificēti, risku modelis ir izstrādāts, ka arī izstrādātas rekomendācijas risku mazināšanai. Pētījuma mērķis ir sasniegts.

Summary

The purpose of the study is to perform a risk analysis using the loan comparison platform. To achieve the goal, the following objectives were set: (1) to classify potential IT risks; (2) to develop a CORAS risk model; (3) to develop risk reduction recommendations. The loan comparison platform is an information system through which lenders and borrowers can successfully cooperate and fulfill their tasks and roles. On this platform, any prospective borrower can complete a loan comparison application form and receive loan offers from various lenders. Three participants are involved in the process: a client, a platform consultant and a lender. Project risks were identified using the CORAS method (see Table 1) and the risk analysis chart was constructed using the CORAS software (see Figure 2). If the customer accidentally or intentionally enters incorrect information, this may lead to the fact that the credit application will not be processed. In turn, this can lead to a loss of client trust and a decrease in the number of customers. Platform Consultant carries the most risks. His/her unprofessionalism may be the cause of poor-quality consultation and non-compliance with internal procedures may lead to the fact that the loan application will not be processed on time and the client will be lost. Both the platform consultant and the lender have access to customer data, which creates a risk associated with the transfer of data to a third party. Data can be used for other purposes, what is illegal and leads to a loss of financial and customer confidence. Technologies are also fraught with risks, since software errors and viruses can interfere with normal operation. As a result, client applications can not be processed in a timely manner. The next step is to identify or develop a set of actions that can reduce the likelihood of each incident. For example, regular computer maintenance can reduce the probability of damage to zero percent. Regular training of consultants and passing tests can improve the quality of client advice. Risk analysis is the continuous and systematic work of each project. Therefore, the risk analysis chart can be added with new risk incidents and risk mitigation measures during the project.

Literatūra

1. Business Process Model and Notation (BPMN) January, 2011. <https://www.omg.org/spec/BPMN/2.0/PDF>
2. Dimitrakos T.. (January 2002). CORAS, A Platform for Risk Analysis of Security Critical Systems sk.internetā 27.12.2020 [https://www.researchgate.net/publication/30418730_CORAS -
_A Framework for Risk Analysis of Security Critical Systems](https://www.researchgate.net/publication/30418730_CORAS_-_A_Framework_for_Risk_Analysis_of_Security_Critical_Systems)
3. CORAS Tool 2.0 programma <http://coras.sourceforge.net/downloads.html>
- 4.B,Folken SINTEF, The CORAS model-based Method for security risk analysis [https://www.uio.no/studier/emner/matnat/ifi/INF5150/h06/undervisningsmateriale/060930.CORAS-handbook-
v1.0.pdf](https://www.uio.no/studier/emner/matnat/ifi/INF5150/h06/undervisningsmateriale/060930.CORAS-handbook-v1.0.pdf)
- 5.Faizulajev D. МЕТОДЫ И СРЕДСТВА АНАЛИЗА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ <https://core.ac.uk/download/pdf/208322484.pdf>
6. Stolen K., Guided Tour of the CORAS Method https://www.researchgate.net/publication/287673426_A_Guided_Tour_of_the_CORAS_Method