PAMETNA KASICA

Juraj Nöthig

Filip Lončarić

Antonio Janach

Visoko učilište Algebra, Ilica 242, Zagreb, Hrvatska

SAŽETAK

Sustav za poticanje štednje koji nije invazivan, kojeg korisnik stvarno smatra korisnim dijelom njegovog života je nešto čega trenutno nema dovoljno na tržištu. Time smo odlučili kreirati sustav pametne kasice koji bi motivirao korisnika na štednju povezivanjem jednog jednostavnog koncepta štednje s modernim tehnologijama. Sam sustav bi se sastojao od mobilne aplikacije povezane s pametnom kasicom, mobilna aplikacija bi komunicirala sa serverom koji sadržava sve potrebne podatke u bazi podataka. Sve ćemo dostatno zaštiti s obzirom na to da se ovdje radi o informacijama u nečijem novcu i analizirati rizike za naše uspješno poslovanje.

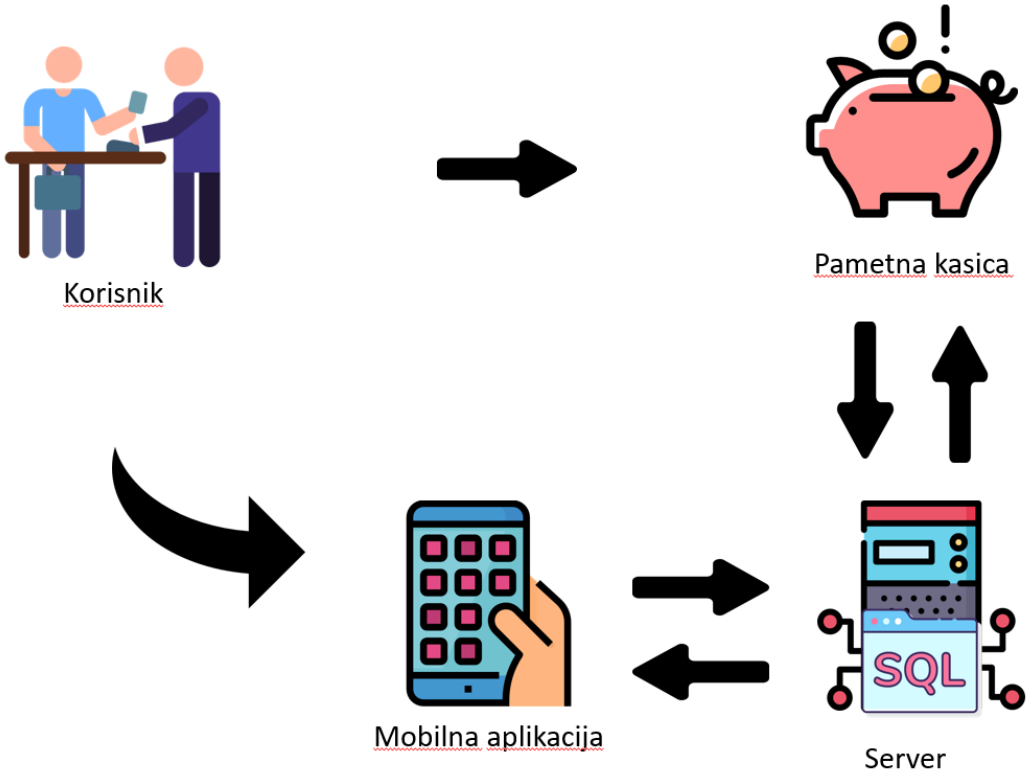
Ključne riječi: pametna kasica, štednja, baza podataka, aplikacija, server, informacijski sustav, motivacija, korisnik, administrator, programer, zaposlenik, dizajner, mobitel, internet, novac, proces

1. SUSTAV

1.1 Opis sustava

Pametna kasica ima svrhu motivatora na štednju. Motivaciju korisnika bi postigli putem mobilne aplikacije gdje bi korisnik odredio svotu koju želi uštedjeti, kasica se tada zaključa i nije je moguće otključati sve dok god korisnik ne sakupi željeni iznos. Pametna kasica bi se našla u širokoj primjeni u bankama, školama, ostalim obrazovnim institucijama i domovima. Kasica bi našla primjenu u bankama na svakom pultu gdje se obavljaju transakcije za plaćanje ili umjesto običnih kutijica koje su postavljene za ubacivanje kovanica za Caritas. Pametna kasica bi bila povezana s evidencijskim sustavom koji bi objavljivao rezultate prikupljenih sredstava na web stranici Caritasa tako da korisnici mogu vidjeti kome je njihova specifična donacija pomogla. Gledajući kasica ima primjenu i u školama gdje bi svaki razred mogao sakupljati razredni novac za maturalne izlete, pomoć djeci siromašnih roditelja ili bilo koje druge potrebe unutar razreda. U pametnu kasicu bi ubacivali novac i sakupljali, a rezultati bi bili vidljivi svakom učeniku na njegovom mobilnom telefonu putem aplikacije i time ih poticali na naviku štednje i u osobnom životu. Kućna upotreba bi u ovom slučaju bila najjednostavnija gdje bi korisnik štedio za svoje osobne potrebe, a aplikacija pametne kasice bi ga dnevno ili tjedno obavještavala o stanju sredstava i time motivirala da i dalje ubacuje novac kako bi došao do svog cilja. Ostale mogućnosti koje bi bile ugrađene u kasicu su ugrađena jednostavna budilica i sat povezana aplikacijom, svjetlo koje bi moglo poslužiti za noćni ormarić. Praćenje stanja novaca pomoću mobilne aplikacije, senzor za prepoznavanje valute novca koji ima mogućnosti razlikovanja između papirnatog i novca u kovanicama.

1.2 Elementi sustava



Korisnik putem mobilne aplikacije zadaje iznos koji želi uštedjeti, zatim se taj parametar posprema u bazu podataka koja se pokreće na nekom serveru. Nakon što se promjena zapiše u bazu podataka pametna kasica čita tu promjenu nad tim parametrom. Kad je kasica pročitala tu promjenu ona se zaključava. Za vrijeme dok je kasica zaključana korisnik ubacuje novac gdje pametna kasica taj novac zbraja i svoj parametar o trenutnom stanju šalje prema bazi podataka. Kad se taj podatak zapiše mobilna aplikacija dohvaća taj podatak i ispisuje trenutno stanje na mobilnoj aplikaciji gdje korisnik može pročitati trenutno stanje kasice. Kad korisnik ispuni svoj cilj ili više od toga kasica se otključava i korisnik može izvaditi ušteđenu količinu novca koju je prethodno zadao.

Time se sustav sastoji od korisnika koji svojim radnjama aktivira štednju na mobilnom uređaju u mobilnoj aplikaciji koji šalje podatke prema SQL serveru i kasice koja prima taj podatak i po njemu se zaključava.

2. PROCES

2.1 Opis ključnog procesa

Kao što je prethodno spomenuto u točki Elementi Sustava, kasica se sastoji od 4 ključna elementa, a to su korisnik, pametna kasica s upravljačem, mobilna aplikacija i server na kojem je baza podataka iz koje kasica zapisuje i pohranjuje parametre. Na serveru se također nalazi poslužiteljska strana aplikacije koja uslužuje mobilnu klijentsku aplikaciju. U sljedećem dijelu detaljno se opisuje kako proces kasice funkcionira i kako je strukturiran skup aktivnosti za ostvarenje cilja uštede novca kod korisnika kao i sam ciklus ponavljanja.

Korisnik pomoću mobilne aplikacije zadaje cilj uštede koji želi ostvariti. Mobilna aplikacija šalje parametar dostupnim Internet linkom prema serveru. Server prima parametre i aplikacija

ih unosi u bazu podataka, postavlja ih kao zadnji cilj i šalje prema mobilnoj aplikaciji potvrdu unosa. Upravljač u kasici čita tu promjenu putem bluetooth veze i zaključava kasicu.

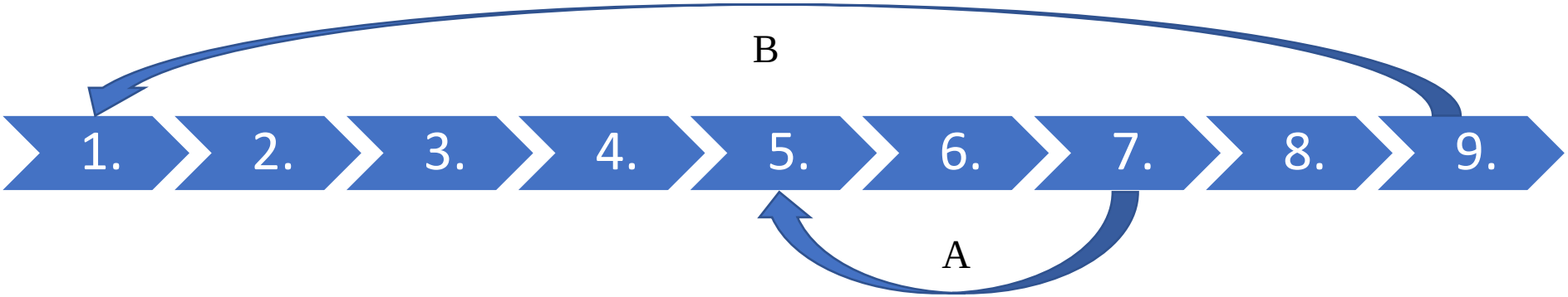
Korisnik ubacuje novac u kasicu proizvoljno, kasica na vrhu svog kućišta ima dva utora za ubacivanje novaca, jedan utor za ubacivanje kovanica i jedan utor za ubacivanje novčanica. Pri vrhu kućišta gdje se nalazi utor je ugrađen uređaj koji ima u sebi senzor. Senzor skenira i prepoznaje o kojoj kovanici ili novčanici je riječ. Kad senzor skenira on predaje vrijednost upravljaču tako da na trenutnu vrijednost zbroji vrijednost koja je dodana kovanicama ili novčanicama. Svaki puta kad korisnik ubacivanjem kovanice ili novčanice ekvivalentna se vrijednost prosljeđuje prema mobilnoj aplikaciji koja taj parametar proslijedi poslužiteljskoj aplikaciji na serveru. Mobilna aplikacija taj parametar šalje pomoću internetske veze serveru. Kad mobilna aplikacija taj parametar pošalje serveru, server taj unos upisuje u bazu podataka i šalje taj podatak pomoću internetske veze mobilnoj aplikaciji na mobitelu u obliku obavijesti. Slanje parametra između mobilne aplikacije i servera označava međusobnu komunikaciju kako bi parametri za prikaz trenutnog stanja bili prikazani u stvarnom vremenu. Kad server pošalje podatak u kojem javlja trenutno stanje štednje mobilna aplikacija prikazuje u svojem sučelju prikaz o napretku prema cilju štednje i prikaz stanja koliko korisnik još mora uštedjeti da bi ostavio svoj cilj. Kontinuiranim ubacivanjem novca kasica se puni do trenutka kad vrijednost novca ne dosegne zadanu vrijednost. Zadana vrijednost je definirana prije početka štednje a pritom zadana vrijednost štednje označava svotu koju korisnik želi ispuniti. Kad korisnik dosegne zadanu vrijednost kasica se otključava. Kad se otključa mobilna aplikacija šalje notifikaciju o uspješnoj štednji.

2.2 Ciklički proces štednje

Kako bi se korisnika navelo da uštedi što više, mobilna aplikacija javlja da je kasica spremna za restart ciklusa štednje. Po završetku prošlog ciklusa šalje se notifikacija koja obavještava korisnika da može pokupiti prikupljen novac i ponovno postaviti novi cilj. Kada korisnik postavi novi cilj, poslužiteljska strana aplikacije na serveru pokreće novi ciklus, unosi potrebne podatke u bazu podataka i javlja mobilnoj aplikaciji da je pokrenut novi ciklus štednje. Mobilna aplikacija šalje kasici podatak i ona se ponovno zaključava.

Nakon svakog ciklusa se u bazi podataka otvara novi unos, a svi prijašnji unosi se pohranjuju i imenuju datumom i vremenom početka i kraja. Ti podaci se uspoređuju s podacima drugih korisnika i za one koji su natjecateljskog duha, mogu služiti uspoređivanju s drugima tako da kod svake štednje upišu što su napravili sa sredstvima koje su prikupili.

2.3 Skica ključnog procesa



1. Postavljanje cilja štednje u mobilnoj aplikaciji
2. Server prima informaciju i zapisuje ju u bazu podataka
3. Server šalje potvrdu o novoj štednji prema mobilnoj aplikaciji
4. Aplikacija zaključava odabir, šalje kasici putem bluetootha, kasica prihvaća odabir i zaključava se
5. Ubacivanjem novaca se aktivira senzor u kasici koji šalje vrijednost mobilnoj aplikaciji
6. Mobilna aplikacija prosljeđuje unos serveru
7. Server zapiše vrijednost i čeka idući unos
8. Po dosegu cilja šalje notifikaciju i signal kasici preko mobitela o završenoj štednji
9. Otključavanje kasice po dosizanju cilja i preuzimanje štednje

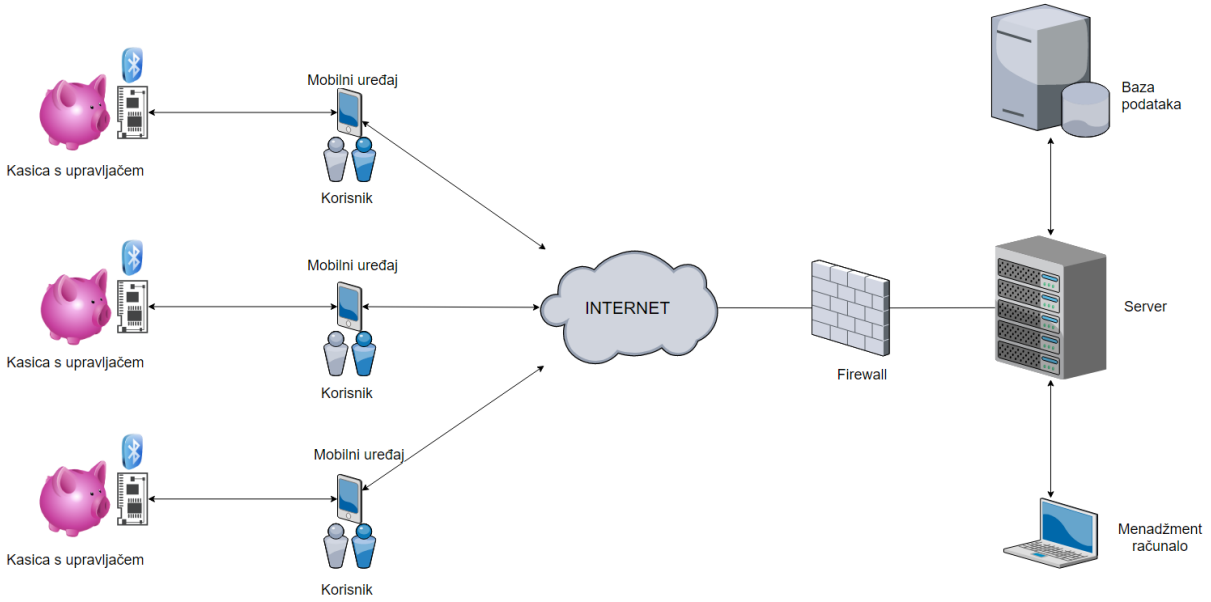
A - ubacivanje novca u kasicu, ciklus koji se ponavlja dok se ne dođe do zadanog cilja

B - ponovno pokretanje ciklusa štednje

3. INFORMACIJSKI SUSTAV

3.1 Hardware

- Kasica - građena je od keramike kako bi korisnici dala osjećaj prave starinske kasice u obliku svinjice, visoka je od 30-50 cm ovisno o tome koju korisnik naruči (2 modela), te je širine 10-20 cm, rupa na vrhu promjera za kovanicu od 25 kn, te još jedna rupa za novčanice (10, 20, 50, 100, 200, 500, 1000 novčanice)
- Kontroler - ugrađen je na vrh kasice te je na njega također dodan senzor. Kontroler drži program u kojem zadajemo koliko želimo uštedjeti I ovisno o tome on će javljati serveru da je cilj zadovoljen, koliko još treba do cilja, koliko prosječno štedimo na dan/tjedan/mjesec/godinu
  Kontroleri koje ćemo koristiti su Arduino i MicroBit
- Server - infrastruktura će se podignuti na jednom serveru sa sljedećim specifikacijama i postaviti pristup internetu s odgovarajućim tehnologijama
  Specifikacije: HP DL380p Gen8 G8 XEON SIX, 2 x Intel Xeon E5-2600, 128 GB RAM, 8 TB HDD x2
- Senzor - osjetilni senzor koji ima mogućnost prepoznavanja kovanica i novčanica
- Kutija i žice - povezivanje sklopova i zaštitno kućište za kontrolere
- Napajanje - napajanje za kontroler, senzor za kovanice i elektromagnetsku bravu
- Elektromagnetska brava - sustav zaključavanja kasice
- Indikatori (LED lampica, dioda) - jednostavni prikaz modova rada kontrolera



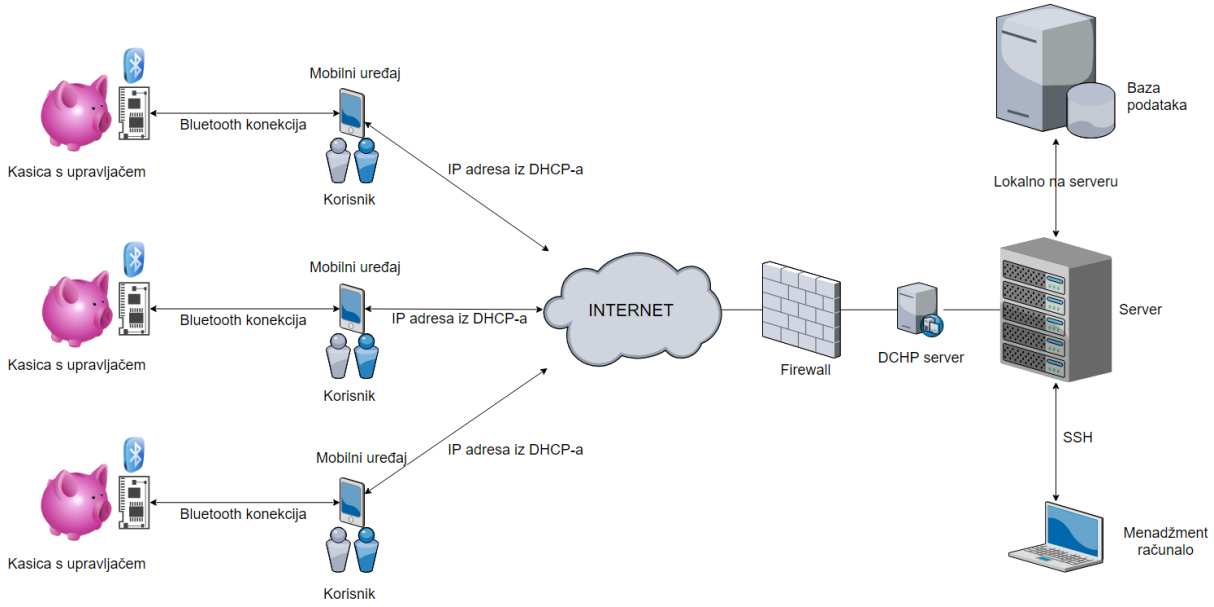
3.2 Software

- Poslužiteljska strana aplikacije - aplikacijska platforma gdje administratori mogu upravljati sklopovljem putem internetske veze web sučeljem, rješavati eventualne probleme korisnika koje su dobili putem sustava za podršku korisnika, također informacije kao ukupno uštađeno ovim putem, ukupan broj korisnika i njihov status, statistiku korištenih kovanica i novčanica
- Mobilna aplikacija - klijentska strana aplikacije koja će biti dostupna za preuzeti preko interneta na korisnički mobilni uređaj, omogućuje evidenciju, postavljanje i

modifikaciju postavki kasice i korisničkog računa na serveru, prijava na sustav će se obavljati prijavom e-mail adresom i passwordom, MFA po izboru

3.3 Netware

- Javna mrežna infrastruktura - mrežna infrastruktura koju koriste poslužiteljska i klijentska strana za komunikaciju će biti link prema internetu za poslužitelj i mobilna LTE 4G konekcija za klijentske mobilne uređaje
- Firewall - zaštita od neželjenog pristupa i sigurnosnih rizika za podatke na serveru i bazi podataka
- LTE - mobilni uređaji pretežito koriste mobilnu LTE 4G mrežu za pristup infrastrukturi
- Bluetooth - kasica će se povezivati na mobitel bluetooth tehnologijom i klijentsku aplikaciju koja dalje šalje informacije serveru
- Upravljač na kasici - mogućnost spajanja bluetooth tehnologijom na mobilni uređaj, MAC adresa i odašiljač
- Usmjernik - usmjeruje promet s interneta od korisnika do servera, svaki korisnik će dobiti privremenu IP adresu DHCP-om pri uspostavljanju konekcije do završetka session-a, tj. do kraja prijenosa podataka
- SSH - za potrebe administracije servera potreban je SSH konekcija kako bi osigurali sigurnu konekciju
- VPN - kako bi osigurali pristup korisnicima koji imaju striktnija pravila pristupa internetu, bit će im osiguran VPN pristup serveru putem mobilne aplikacije
- DHCP server - za dodjelu adresa klijentskim aplikacijama instaliran je DHCP server koji automatski dodjeljuje IP adrese svakom klijentu koji zatraži vezu sa serverom



3.4 Dataware

- Baza podataka - jednostavna SQL baza podataka koja sortira podatke u kategorije za svakog korisnika kao što su osobni podaci, štednje, datumi, statistički podaci
- Notifikacije - obavijesti za korisnika o stanju u kasici i napretku štednje

3.5 Lifeware

- Korisnik - osoba koja koristi sustav u svrhu osobne štednje

- Programer - zaposlenik koji po dizajnu programira poslužiteljsku aplikaciju i klijentsku aplikaciju
- Sistemaš - zaposlenik koji postavlja i uređuje serversku i mrežnu infrastrukturu
- Dizajner - dizajnira frontend klijentskog aplikacijskog sučelja i dio backenda aplikacije
- Administrator - osoba koja se brine o funkcioniranju i održavanju infrastrukture

3.6 Orgware

- Proces nadogradnji - putem mobilnog distribucijskog sustava slale bi se nadogradnje za klijentsku aplikaciju kako bi se održala kvaliteta usluge
- Pregled logova - serverska strana će sadržavati detaljan logging sustav po kojem će se moći pronaći i identificirati problemi unutar infrastrukture i aplikacije
- Sigurnosne procedure - zaštita od curenja podataka i dodjela prava
- Backup - pohrana sigurnosnih kopija baze podataka i cijele serverske infrastrukture u slučaju ne rješivih problema
- Call support - 24/7 podrška za korisnike usluga

4. SIGURNOST INFORMACIJSKOG SUSTAVA

4.1 Opis primijenjene mjere zaštite informacijskog sustava

4.1.1 Lozinka

Sve lozinke koje služe za pristup infrastrukturi će morati slijediti pravilo kompleksnosti od minimalno 12 znakova, minimalno 2 velika slova, 2 specijalna znaka i brojevi. Korisnici neće smjeti koristiti ikakve osobne podatke u lozinki, provjera lozinke će biti odrađena na osnovu unesenih osobnih podataka i slikane osobne kartice. Potreba za mijenjanjem lozinke će biti produžena na godinu dana umjesto standardnih 3 mjeseca jer je veća šansa da korisnik stavi slabiju lozinku ako ju mora često mijenjati. Također neće biti sustava hintova i tajnih pitanja.

4.1.2 MFA

Multi-factor autentikacija za klijente će biti omogućena pomoću već poznatih mobilnih *authenticator* aplikacija ili SMS-om. Postavljena lozinka će biti i dalje potrebna za pristup korisničkim računima.

Za pristup s administratorske strane, tj. administratorskom accountu će biti postavljena trostruka MFA koja će se sastojati od lozinke, koda s *authenticator* aplikacije i otiska prsta poznatog u bazi. Za otisak prsta će se koristiti posebni skeneri autorizirani samo za naš server.

4.1.3 Fizički pristup serverskoj sobi - kartica/otisak prsta, kamere

Serverska soba će biti zaštićena višestrukom fizičkom autentikacijom. Kod ulaza je potrebno imati autoriziranu pristupnu karticu, otisak prsta koji je unesen u bazu podataka i prepoznavanje lica sustavom nadzora.

4.1.4 Zaštita od nedozvoljenog pristupa (Firewall, enkripcija, dozvole)

Prilikom nedozvoljenog pristupa, napada izvana putem interneta, presretanjem prometa ili zlonamjernog pristupa od strane zaposlenika će se uspostaviti zaštita u obliku firewalla, enkripcije podataka tijekom slanja putem mreže i postavljanjem dozvola pristupa za svakog radnika.

Firewall će biti hardverskog tipa spojen na server i nadzirat će sav promet koji prolazi kroz njega po određenim pravilima.

Enkripcija podataka će biti omogućena AES256 algoritmom.

Dozvole pristupa će biti podijeljene u 3 tipa:

- Administrator - pristup platformi s kojom administriramo serversku stranu aplikacije i korisničke aplikacije
- Podrška - zaposlenici koji poznaju sustav, ali nemaju prava mijenjati išta na sustavu nego samo prijavljivati aktualne probleme
- Klijenti - korisnik koji ima pristup samo vlastitim podacima i upravljanu istih

4.1.5 Backup procedura

Sigurnosna pohrana cijelog servera koja će nam omogućiti oporavak u slučaju gubitaka podataka ili napada izvana. Svaki tjedan će se obavljati backup cijelog servera i sigurnosne kopije će se čuvati mjesec dana unatrag. Svaki dan u vrijeme najmanje aktivnosti servera će se odrađivati diferencijalni backup i inkrementalni svakih sat vremena.

Ako dođe do potrebe za povratom podataka to će se moći odraditi s minimalnim *down timeom* bez gubljenja podataka.

4.1.6 Zaštita od prirodnih katastrofa i nepogoda (potres, požar, poplava)

Kao zaštitu od prirodnih nepogoda ćemo instalirati server u IoSafe kućištu. IoSafe Server 5[1] model ima mogućnost sačuvati podatke od požara (30 min), poplave (3 dana) i dolazi s protuprovalnim kućištem. Kao zaštitu od potresa server će biti postavljen u novu anti-potresnu sobu koja može izdržati potres do 7 jačine po Richteru.

4.2 Osvještavanje zaposlenika

Zaposlenici su jedan od najvećih rizika za informacijsku sigurnost tvrtke. Njihovo znanje i poznavanje sustava u kojem rade je ključno za izbjegavanje velikih sigurnosnih propusta. Stoga je potrebno informacijsku sigurnost približiti svim zaposlenicima, i to ne samo u svrhu zaštite i povećanja sigurnosti, nego i poboljšanja komunikacije između osoblja. Rješenje za takav problem je organizirana edukacija cjelokupnog osoblja o najčešćim mogućim propustima zaposlenika.

U tu kategoriju spadaju napadi tipa *USB dropping*, gdje se namjerno ostavljanje USB stickova na lokacijama gdje prolaze zaposlenici koji na sebi sadrže program koji se aktivira pri uključivanju u bilo koje računalo. Zaposlenike bi se time učilo kako isključiti *AutoRun* opciju na svim računalima na kojima rade, a koja nisu dio službene infrastrukture i da svoje „pronalaske“ ne testiraju u tvrtki.

Također ćemo obratiti pozornosti na razne vrste malicioznih stranica, lažnih marketinških materijala i vrste malicioznih programa koje se mogu na njima pokupiti. Neki od tipova su *ransomware*, *malware*, *bloatware*, *cryptojacking*, *trojan* i ostali. Većina samo usporuje rad računala do nefunkcionalnih razina i smanjuje produktivnost ili briše podatke, dok *ransomware* zaključava sve podatke koje vidi nekom enkripcijom i traži otkupninu i time se svrstava u najopasnije.

Kategorija koja spada malo više u *social engineering* je takozvani *phishing*. Obično se šalju mailovi naslovljeni na vaše ime u kojem se navodi da je osvojena neka nagrada ili da je potrebno predati podatke za primitak plaće za ovaj mjesec ili slično, gdje se dolazi do osobnih podataka

[1] https://iosafe.com/products/server-5/

ili pristupa na računala unutar tvrtke. Među takvim napadima se nalaze i lažni zahtjevi za promjenu lozinke, prilikom koje se mora upisati i trenutna lozinka.

Edukacija bi se svodila na gledanje edukacijskih videa i održanih prezentacija za sve zaposlenike nakon čega bi održali simulaciju prepoznavanja lažnih zahtjeva. Navela bi se pravila pisanja pravilne, čvrste lozinke i postavila pravila o zabrani pisanja i zapisivanja te lozinke igdje lako dostupno. Tijekom rada zaposlenicima bi se jednom mjesečno poslao lažni mail kao testiranje usvojenosti, a i koncentracije na posao.

Nakon uspješno provedenih edukacija i testiranja, šanse za neovlašteni pristup će biti višestruko umanjene i poslovanje olakšano. Moći ćemo se osloniti na zaposlenike više i povjerenje unutar tvrtke će se povećati.

5. UPRAVLJANJE RIZICIMA

5.1 Procjena rizika

Proces procjene rizika se sastoji od:

- Identifikacija rizika – traženje, prepoznavanje i opis rizičnih dijelova našeg sustava te ako je nešto rizik ili ne, moguće uzroke i posljedice
- Analiza rizika – proučavanje rizičnog dijela ili dijelova te razumijevanje rizika i odredba visine rizika
- Vrednovanje rizika – pridavanje veće ili manje vrijednosti određenim rizicima

1. Poplava

UZROK: neispravne vodovodne instalacije, neispravne protupožarne instalacije, loše izolirana sistem sala od prirodnih nepogoda

MOGUĆE POSLJEDICE: uništena oprema u sistem Sali zajedno sa diskovima i podacima, financijski gubitci

2. Potres veći od 6.0 po Richteru

UZROK: prirodna nepogoda, nepredvidiv događaj

MOGUĆE POSLJEDICE: nedostupnost usluge zbog pada servera, urušavanja zgrade, prekid interneta, smrskane opreme

3. Manjak sigurnosnih zakrpi OS-a

UZROK: zakrpe koje nisu instalirane pravovremeno zbog lijenosti ili zaborava

MOGUĆE POSLJEDICE: sigurnosna rupa koja oslabljuje sigurnost cijelog sustava i izlaže sustav probojima izvana

4. Nestručnost zaposlenika

UZROK: manjak obrazovanja i želje za učenje kao i motivacija za radom kod zaposlenika

MOGUĆE POSLJEDICE: moguć upad „social engineeringom“ tipa USB droppom, loše zaporke, loše ili slabo postavljena sigurnosna infrastruktura, nesvjesnost o pogrešci i ignoriranje

5. **Kvar hardwarea (serverska oprema)**

UZROK: stari i dugo korišteni hardware, slabo održavanje hardware-a i neredoviti servis

MOGUĆE POSLJEDICE: ispad dijela infrastrukture iz funkcije, financijska oštećenja gubitkom vremena

6. **Ransomware**

UZROK: loše postavljena sigurnosna zaštita infrastrukture, loše informatičko obrazovani zaposlenici

MOGUĆE POSLJEDICE: zaključani svi podaci u infrastrukturi, nedostupnost podacima, zaražena sigurnosna kopija

7. **Pad aplikacije**

UZROK: nestabilnost aplikacije, manjak sredstava za ulaganje, nerealni plan dodanih funkcija, nedovoljno testiranje aplikacije

MOGUĆE POSLJEDICE: rušenje aplikacije, nezadovoljni korisnici, komplicirano sučelje, neprivlačan estetski dizajn

8. **Bolovanje zaposlenika (COVID-19)**

UZROK: prirodna nepogoda, nepredvidljiv vektor, slaba osviještenost zaposlenika o higijeni

MOGUĆE POSLJEDICE: višestruka bolovanja, nemogućnost funkcioniranja tvrtke i usluge, financijski gubici

9. **Nestanak struje**

UZROK: instalacije loše kvalitete, kratki spoj, radovi na distribuciji strujne mreže, napajanja loše kvalitete, pad strujne infrastrukture HEP-a

MOGUĆE POSLJEDICE: korumpirani podaci, gubitak podataka, prestanak rada usluge

10. **Jedan ISP**

UZROK: loša procjena infrastrukturnih zahtjeva i zahtjeva usluge i korisnika, nedostupnost drugog ISP na tom području

MOGUĆE POSLJEDICE: pad usluge i nedostupnost servera, financijski gubici,

5.2 Matrica vjerojatnost-utjecaj

Utjecaj			
	2. 9.	6.	7.
	1. 4.	3. 5.	8.
			10.
	Vjerojatnost		

5.3 Postupanje s rizicima

1. Poplava

Serverska soba će biti postavljena na drugi kat zgrade gdje poplavne vode ne mogu doseći. Sama soba će biti konstruirana bez provedenih cijevi s tekućom vodom u zidovima ili stropu iznad same sobe, kvalitetno izolirana u slučaju kvara vodovodnih cijevi. Također sam hardware servera je u vodonepropusnom kućištu.

2. Potres veći od 6.0 po Richteru

Server postavljen u zgradi novije građe otporne na jače potrese i armiranom serverskom sobom.

3. Manjak sigurnosnih zakrpi

Obrazovani sistemaši koji razumiju bitnost zakrpi i po potrebi obrazovanje istih, redovita instalacija novih zakrpi na sustav i po mogućnosti mailing sustav za obavještavanje o dostupnosti novih zakrpa.

4. Nestručnost zaposlenika

Detaljan razgovor za posao, dodatno obrazovanje zaposlenika, zapošljavanje stručnijeg osoblja koje može poslužiti u svrhu mentoriranja. Postavljena stroža pristupna pravila kategorizirana po iskustvu zaposlenika.

5. **Kvar hardwarea (serverska oprema)**

Redovan servis i održavanje opreme, kupnja rezervnog i kvalitetnijeg hardware-a, kupnja i instalacija kvalitetnih programa za dijagnostiku.

6. **Ransomware**

Edukacija zaposlenika o mogućim prijetnjama i organizacija testiranja osoblja lažnim phishing mailovima. Odvojena infrastruktura za pohranu sigurnosnih kopija sustava (backup sustav), ograničen pristup infrastrukturi u kritičnim pristupnim točkama, ograničen broj autoriziranih osoba za adminski pristup.

7. **Pad aplikacije**

Više uloženog vremena i sredstava u testiranje stabilnosti aplikacije, zaposliti kvalitetnije programere i dizajnere na kraći period za vrijeme aktivnog razvoja.

8. **Bolovanje zaposlenika (COVID-19)**

Osviještenost o stanju u svijetu, poboljšanje higijene na radnom mjestu, smanjenje fizičkog kontakta među zaposlenicima, izolirana radna mjesta, mogućnost rada od kuće.

9. **Nestanak struje**

Postavljen UPS dovoljne jačine i kapaciteta da održi server u operativnom stanju 6 sati. Procedura za pospremanje svih podataka i normalno gašenje infrastrukture kada je UPS pri kraju svojeg kapaciteta.

10. **Jedan ISP**

Ulaganje u drugi ISP sa svrhom postizanja redundancije pristupa internetu.

6. ZAKLJUČAK

Izrada sustava koji ima sve potrebne elemente pokrivene, definirane i razrađene je dugotrajan proces kojem treba dati dovoljno vremena da se dovrši. IT sustavi po tome nisu ništa drugačiji osim činjenice da je većina toga neopipljivo i time je potrebna veća doza razumijevanja kako bi se takav projekt pravilno osmislio i izvršio.

Početak svakog projekta je najbitnija stavka jer o njoj ovisi najviše budućeg planiranja, time smo na početku definirali elemente sustava i opisali njihovu osnovnu funkciju. Svaki od elemenata sudjeluje u nekom od procesa koji se odvijaju kako bi u našem slučaju cilj štednje kod korisnika bio postignut. Time smo definirali sve ključne procese, objasnili ih i postavili u tijek koji definira ciklički proces štednje kao i skicu procesa.

Svaki automatizirani proces zahtjeva neki oblik razmjene informacija koje se kreću kroz dijelove sustava kako bi došle do svojeg odredišta i postigle neki zapis, aktivaciju, deaktivaciju ili potvrdu u sustavu. Taj dio sustava se zove informacijski sustav i za njega smo definirali sve dijelove koji spadaju u kategorije hardware, software, netware, dataware, lifeware i orgware.

Također, informacijski sustav mora biti siguran tijekom izvođenja svojih operacija čime se bavimo u poglavlju sigurnosti informacijskih sustava. Svaki kritični dio informacijskog sustava je potrebno zaštiti od nedozvoljenog pristupa, nehotičnih postupaka prouzročenim neznanjem i

postaviti sigurnosnu kopiju koja će omogućiti povrat u bilo koji trenutak. U mjere opreza se ubrajaju i znanja i iskustvo samih zaposlenika koji rade sa sustavom gdje smo se odlučili na edukaciju i testiranje njihove povjerljivosti kako bi se utvrdila slaba točka u sustavu ili zaposlenicima.

Iako je sigurnost nekog sustava na razini, ipak je potrebno definirati, analizirati i procijeniti moguće rizike. Time se radi upravljanje rizicima gdje definiramo najutjecajnije rizike na naš sustav, ocjenjujemo ih u pomoću matrice vjerojatnosti i utjecaja, te na kraju postavljamo naše postupanje s pojedinim rizikom unutar naših mogućnosti gdje dio rizika prihvaćamo, a dio umanjujemo svojom odlukom i postupcima.