UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

ZAKLJUČNA STROKOVNA NALOGA VISOKE POSLOVNE ŠOLE

VARNOST SPLETNEGA POSLOVANJA NA PRIMERU SPLETNE TRGOVINE SKYGURU

Ljubljana, september 2016 PETER MIKLAVČIČ

IZJAVA O AVTORSTVU

Podpisani Peter Miklavčič, študent Ekonomske fakultete Univerze v Ljubljani, avtor predloženega dela z naslovom Varnost spletnega poslovanja na primeru spletne trgovine SkyGuru, pripravljenega v sodelovanju s svetovalcem dr. Anton Manfreda.

IZJAVLJAM

1. da sem predloženo delo pripravil/-a samostojno;

2. da je tiskana oblika predloženega dela istovetna njegovi elektronski obliki;

3. da je besedilo predloženega dela jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem poskrbel/-a, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam oziroma navajam v besedilu, citirana oziroma povzeta v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani;

4. da se zavedam, da je plagiatorstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku Republike Slovenije;

5. da se zavedam posledic, ki bi jih na osnovi predloženega dela dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom;

6. da sem pridobil/-a vsa potrebna dovoljenja za uporabo podatkov in avtorskih del v predloženem delu in jih v njem jasno označil/-a;

7. da sem pri pripravi predloženega dela ravnal/-a v skladu z etičnimi načeli in, kjer je to potrebno, za raziskavo pridobil/-a soglasje etične komisije;

8. da soglašam, da se elektronska oblika predloženega dela uporabi za preverjanje podobnosti vsebine z drugimi deli s programsko opremo za preverjanje podobnosti vsebine, ki je povezana s študijskim informacijskim sistemom članice;

9. da na Univerzo v Ljubljani neodplačno, neizključno, prostorsko in časovno neomejeno prenašam pravico shranitve predloženega dela v elektronski obliki, pravico reproduciranja ter pravico dajanja predloženega dela na voljo javnosti na svetovnem spletu preko Repozitorija Univerze v Ljubljani;

10. da hkrati z objavo predloženega dela dovoljujem objavo svojih osebnih podatkov, ki so navedeni v njem in v tej izjavi.

V Ljubljani, dne _____ Podpis:_____

KAZALO

UVOD

Od samega pojava interneta oziroma spleta, ki je bil sprva namenjen le enostavnemu komuniciranju, so se pojavljali tudi ljudje, ki so hoteli z njim služiti. Z internetom so se odprle povsem nove možnosti trgovanja in se tako vpletle v svetovno gospodarstvo, da si danes poslovanja brez njega praktično ne znamo predstavljati. Upira se mu praktično samo blagovna menjava in nekaj gotovinskega prometa. Skoraj vsak nakup ali transakcija je zabeležena v neki računalniški obliki in skoraj vse se pretaka oziroma premika in shranjuje med vpletenimi strankami preko svetovnega spleta.

Kjer pa se pojavi možnost trgovanja in zaslužka, se vedno pojavi tudi nekdo, ki se hoče s tem nelegalno okoristiti. Tako so se z razvojem interneta in poslovanja preko spleta razvile tudi kriminalne združbe. Nekoč so denar kradli z noži in pištolami, danes to počnejo preko spleta izza osebnih računalnikov. Kot so se nekoč ljudje poskušali varovati svoj denar z sefi in skritimi prenosi denarja, tako poskušajo tudi danes na varne načine shranjevati in prenašati denar. S pomočjo spletnih bank in bančnih računov, varnih strežnikov, varovanih s požarnimi zidovi in protivirusnimi programi ter varnimi kriptiranimi povezavami.

Še nikoli v zgodovini človeštva malemu podjetniku ni bilo tako lahko prodreti na svetovni trg. Danes je računalnik praktično v vsakem modernem gospodinjstvu, podjetju ali organizaciji, s tem pa tudi poslovni trg in priložnost poslovanja. Za prodor na svetovni trg ni več potrebno imeti ogromnega podjetja z visokimi finančnimi sredstvi, potrebno je le nekaj znanja in dostop do interneta. Podjetnik lahko danes tako rekoč čez noč sodeluje na svetovnem trgu. Z nakupom tehnične in programske opreme lahko podjetnik hitro in z relativno nizkimi stroški posluje z drugimi podjetji ali odpre spletno trgovino in prodaja končnim potrošnikom. Za varnost in prenos transakcij pa skrbijo velike banke in podjetja.

Z idejo poslovanja izven Slovenije smo se soočil tudi sami – predvsem zato, ker je narava naših izdelkov taka, da je Slovenski trg premajhen. Pri prodaji sedežev za letenje z jadralnimi padali se je hitro izkazalo, da bo Slovenija premajhna in da bo potrebno vstopiti na večji trg. Ena možnost je prodaja preko posrednikov, druga pa lastna spletna trgovina. Tako je nastala spletna stran www.skyguru.eu, kjer zdaj teče prva oblika trgovine. Poleg marketinškega vidika, ki je za sam uspeh spletne trgovine izrednega pomena in pomeni njeno dolgoročno preživetje, smo dali velik pomen tudi tehnični izvedbi in varnosti.

V zaključni strokovni nalogi se bom osredotočil na varnost. Predvsem varnost, na katero mora pomisliti mali podjetnik (predvsem slovenski) ob izgradnji spletne trgovine. Tako tehnično varnost spletne strani in vse, kar je povezano z njo: strežniki, brskalniki, požarni zidovi, virusi, kriptiranje in s plačili in njihovo varnostjo. Ob ideji odprtja spletne trgovine Skyguru, so se nam pojavljala številna vprašanja, kako se tehnično lotiti postavitve in predvsem kako poskrbeti za njeno varnost. Kakšne nevarnosti nam pretijo in kako se pred njimi zaščititi. Poskrbeti smo morali za tehnično zaščito računalnika, s katerim opravljamo

vso komunikacijo s kupci in našimi poslovnimi partnerji. Z njim se dostopa, gradi in ureja tudi spletna stran, ki je postavljena na lastni strežnik. Ta je na sedežu podjetja, zato je bilo potrebno poskrbeti tudi za njegovo tehnično varovanje. Poleg tehničnega varovanja prenosa in shranjevana podatkov so nas zanimale tudi možnosti plačil in njihovo varovanje. Pregledali smo predvsem možnosti prejetja plačil, ki jih ima lahko spletna trgovina, postavljena v Sloveniji.

Namen zaključne naloge je predstaviti varnostna tveganja prenosa podatkov in transakcij v spletnih trgovinah. Prikazal bom, kakšne so nevarnosti pri pretoku podatkov in uveljavljene tehnične rešitve. Predstavil bom oblike transakcij, ki jih lahko uporabljajo slovenske spletne trgovine in kako poteka njihovo varovanje. Cilj zaključne naloge je prikazati, na kaj morajo biti pozorni podjetniki pri odpiranju spletne trgovine, da poskrbijo za varnost podatkov in transakcij ter na primeru trgovine Skyguru prikazati tehnične rešitve varovanja prenosa podatkov in transakcij. In predstaviti izboljšave, ki jih bo uvedla.

V prvem delu bo predstavljena tehnična varnost in osnovni pojmi računalniške tehnologije. Kako deluje, kakšne so nevarnosti in kakšno varovanje je potrebno oziroma možno. V drugem delu se bomo osredotočili na načine plačil. Kakšne so možnosti in kako jih zavarovati. V tretjem delu pa bo prikazano varovanje spletne trgovine Skyguru.

1 SPLETNA VARNOST

Pri spletnem trgovanju moramo predvsem poskrbeti za varnost podatkov, ki potekajo med kupcem in prodajalcem. Internet predstavlja precej odprt kanal pretoka informacij, kar predstavlja visoko nevarnost vdora in posledično prevare oziroma zlorabe informacij. Zato moramo poskrbeti tako za varnost spletnih brskalnikov kot varnost računalniške mreže, ki je povezana z računalniškim sistemom. Računalniški sistem predstavlja računalnik, s katerim spletno stran postavimo in jo upravljamo, ter strežnik, na katerem spletna trgovina je.

Kot pri vsaki novi tehnologiji se je tudi pri pojavu interneta in spletnih trgovinah hkrati pojavila tudi zlonamerna stran, ki hoče te stvari zlorabiti.

Vsi dobro zavarovani spletni strežniki, so dnevno bombardirani z več tisoč napadi, od katerih je 99,999 % avtomatiziranih. To pomeni, da je napadalec aplikacija, ki avtomatsko pregleduje in napada spletne strani – trgovine, ki so ranljive ali nezavarovane (Neoserv, 2016a).

Kakor obstajajo različne nevarnosti, tako so se vzporedno razvile tudi različne metode za varovanje pretoka podatkov.

1.1 Nevarnosti spletnega komuniciranja in prenosa podatkov

Pri spletnem komuniciranju in prenosu podatkov gre za prenos podatkov z ene naprave na drugo z uporabo različnih načinov prenosa podatkov, kot so bakrene žice in optična vlakna. Sporočila so sestavljena iz več manjših delov, ki se prenašajo po lokalnih mrežah in javnih omrežji. Pri samem prenosu pa so lahko tarča različnih napadov (Man Young Rhee, 2003, str. 2).

1.1.1 Spletno ribarjenje

Spletno ribarjenje (angl. *Phishing*) je kraja podatkov, ki storilcu omogoča dostop do spletnih strani v imenu žrtve napada. To so lažna spletna mesta, kjer poskuša storilec pridobiti gesla, uporabniška imena ali podatke o kreditnih karticah žrtve in se z njimi naknadno v imenu žrtve prijaviti na spletne strani, kjer se pridobljene podatke zlorabi (Si-Cert, 2016).

Običajno poskušajo z elektronskim sporočilom zvabiti žrtev na lažno spletno stran banke ali spletne trgovine pod pretvezo, da se je potrebno zaradi pomanjkanja podatkov ali dodatnih ugodnosti ponovno prijaviti in preveriti podatke. Če žrtev te podatke vpiše, se ti posredujejo storilcu.

Nevarnosti, oziroma prevari se izognemo tako, da nikoli ne odgovarjamo na elektronska pisma, ki od nas zahtevajo osebne ali finančen podatke ter ne sledimo povezavam takšnih spletnih strani. Osebnih in finančnih podatkov nikoli ne pošiljamo s pomočjo elektronske pošte. Na računalniku moramo imeti vedno nameščene najsodobnejše popravke operacijskega sistema.

1.1.2 Vdor

Vdor je hekerski napad v računalniški sistem, ki se v različnih oblikah pojavi že v 60. in 70. letih prejšnjega stoletja. Gre za nepooblaščen dostop do računalniškega sistema, ki poteka preko slabo zaščitenih oziroma odprtih komunikacijskih vrat, preko katerih se javljajo nanje priključene naprave. Dva najpogostejša načina vdora v računalniški sistem, ki je povezan v omrežje, sta izkoriščanje ranljivosti programa, ki nudi storitev na omrežji, in slabo geslo (Si-Cert, 2016).

Vdoru se najbolje izognemo z rednim posodabljanjem programske opreme in omejevanjem storitev s pomočjo požarnega zidu. Ker se napad preko gesel vrši običajno s uporabo seznama pogostih imen, je potrebno prilagoditi orodja z

omejevanjem najpogostejših lokalno uporabljenih imen. S tem poskrbimo, da so uporabniki naših spletnih trgovin prisiljeni uporabljati kompleksnejša gesla.

1.1.3 Okužbe

Okužba predstavlja programe, katere naj bi uporabniki računalnikov ali strežnikov naložili na svoje sisteme brez vednosti o nevarnosti, ki jih ti povzročajo. Taka programska oprema se lahko pojavlja v različnih oblikah (Neoserv,2016b; MNZ, Policija, 2006; Si-Cert, 2016; Varni na internetu, 2013):

- **zlonamerna koda** (ang. *malware*) je program namenjen povzročanju škode operacijskim sistemom, zbiranju informacij ali vdiranju v operacijske sisteme. Je škodljiv program, ki deluje proti zahtevam uporabnika operacijskega sistema.
- **Virus** je program**,** ki se naseli v operacijski sistem, se sam razmnožuje, prenaša po računalniku in deluje škodljivo z uničevanjem podatkov. Poleg uničevanja podatkov pa so tudi nadležni z izpisovanjem raznih sporočil na zaslone in nepotrebno obremenjujejo računalnik z obremenjevanjem procesorja in polnilnika.
- **Računalniški črv** je zlonamerni program, ki se sam razmnožuje z namenom, da se širi po drugih računalnikih, za kar uporablja internet. Za razmnoževanje v nasprotju z virusom ne potrebuje drugih programov in je namenjen povzročanju škode na internetu. V najboljšem primeru zasedejo samo prostor za razliko od virusov, ki so namenjeni uničevanju oziroma spremembi podatkov.
- **Trojanski konj** je zlonamerni program, ki se predstavlja kot uporabniku prijazen program, v resnici pa deluje v ozadju in povzroča škodo uporabniku. Pogosto deluje kot stranska vrata in omogoča storilcu dostop do žrtvinega operacijskega sistema. Ta lahko pridobiva razne podatke oziroma nalaga druge škodljive programe. Trojanski konj se ne razmnožuje sam in ne spada med viruse.
- **Izsiljevalska koda** (ang. *ransomware*) je zlonamerna koda, ki uporabniku prepreči dostop do računalniškega sistema, dokler ta ne plača odkupnine storilcu – avtorju kode.
- **Nezaželena oglasna pošta** (ang. *spam*) bolj kot okužbo računalnika predstavlja kratenje časa uporabnika. Gre za nezaželeno reklamno sporočilo, ki v večini primerov oglašuje izdelke, navadno dvomljive kvalitete. Lahko povzroča ovire oziroma motenje delovanja operacijskega sistema**.** Nezaželena sporočila v Sloveniji urejata Zakon o elektronskih komunikacijah v 109. členu in Zakon o varstvu potrošnikov v členu 45. a. Zakon določa, da se nezaželene oglasne pošte ne dovoljuje razpošiljati brez vnaprejšnje privolitve prejemnika, razen če se v sporočilu oglašuje podobne izdelke.

1.1.4 Napad z zavračanjem storitev

Napad z zavračanjem storitev (ang. *Denial-of-service attack*) je najresnejši poizkus vdora, ki se izvaja na nivoju celotnega strežnika in ga lahko v najslabšem primeru tudi uniči. Storilec v takih primerih sočasno napade in okuži večje število strežnikov različnih

ponudnikov gostovanj, s katerih nato običajno izvaja napad na večje sisteme, kot so organizacije, podjetja in banke. Več strežnikov se storilec polasti, močnejši je lahko napad. Z dovolj velikim številom strežnikov lahko uniči tudi najbolj zaščitena omrežja. Ti napadi so zelo redki in če je administrator strežnika dovolj pozoren in napad pravočasno opazi, lahko hujše težave tudi prepreči (Rose, 2009).

Aplikacije oziroma programi, s katerimi dostopamo do spleta, so lahko ranljivi tudi zaradi njihove slabe zasnove. To pomeni, da so napadeni preko napak, ki so vgrajene v programu. Storilci izkoriščajo slabo zasnovo programov za vdiranje v sistem. Zaradi tega je izrednega pomena ažurno posodabljanje programske opreme (Causey, 2016).

1.2 Zaščita spletnega komuniciranja in prenosa podatkov

Ker so pri prenosu podatkov preko omrežja – interneta te stalno ogroženi z napadi, moramo poskrbeti za njihovo varnost. Poskrbeti moramo za varnost omrežja z vpeljavo različnih varnostnih protokolov

1.2.1 Omrežna varnostna plast

Omrežna varnostna plast *(ang. Network layer security)* se uporablja za zagotavljanje komunikacij preko skupnih omrežij, kot je internet. Omogočajo zaščito več aplikacij hkrati (Tutorialspoint, 2016).

TCP/IP (ang. *Transmission Control Protocol*) protokol za nadzor prenosa ter IP (ang. *Internet Protocol*) internetni protokol je množica protokolov, ki izvaja protokolski sklad, prek katerega teče internet. Največ omrežnega prometa poteka preko protokola TCP. Sporočila preko protokola TCP, se zaradi vzpostavljene povezave med odjemalcem in servisom prenašajo zanesljivo v obe smeri.

TCP/IP protokoli so lahko varovani s kriptografskimi varnostnimi metodami, med katere uvrščamo SSL (ang. *Secure Sockets Layer*) kriptografski protokol, namenjen vzpostavljanju varnih komunikacijskih povezav, TLS (ang. *Transport Layer Security*) naslednik SSL, PGP enkripcija (ang. *Pretty Good Privacy*) za pošto in IPsec (ang. *Internet Protocol Security*) za omrežno varnost.

1.2.2 SSL in TLS enkripcija

SSL (ang. *Secure Sockets Layer*) je kriptografski protokol namenjen varnemu komuniciranju preko interneta. Nadgrajena oblika SSL je TLS (ang. *Transport Layer Security*). Namenjen je brskanju po spletu, e-pošti, instantnim komuniciranjem in VoIP (ang. *Voice over Internet Protocol*) telefoniji preko internetnega protokola. Med

protokoloma obstajajo majhne razlike, vendar sta v principu enaka (Transport Layer Security, 2016).

Protokol SSL je zelo razširjen povsod, kjer je potreba po prenosu podatkov zaupne narave, kot so osebni podatki in številke kreditnih kartic. Uporablja se pri spletnih trgovinah, spletnemu bančništvu in večjih spletnih straneh, za varovanje komunikacije med strežnikom in spletnim brskalnikom.

SSL je transparenten protokol, ki od končnega uporabnika zahteva malo dela, da ustvari varno povezavo. Pri spletnih brskalnikih so uporabniki opozorjeni na prisotnost SSL protokola s prikazano ključavnico pri naslovu spletne strani.

Navadno so podatki poslani med spletnim brskalnikom in strežnikom v navadni tekstovni obliki kar morebitnim zlonamernim storilcem, ki so te podatke prestregli, omogoča enostaven vpogled. SSL pred pošiljanjem podatke preko interneta kriptira, zato so ob morebitnem prestrezanju ti neuporabni. SSL določa digitalna potrdila in algoritme za kriptiranje, pri katerih se uporabljajo trije ključi (Presentia, 2010b):

- javni ključ, javno znan;
- privatni ključ, pozna samo prejemnik sporočila;
- simetrični ključ, poznata tako prejemnik kot pošiljatelj.

Potek SSL komunikacije (Presentia, 2010a):

- uporabnik preko brskalnika zahteva, da strežnik vzpostavi povezavo preko SLL protokola.
- Strežnik se predstavi z javnim ključem in s tem potrdi svojo pristnost. To poteka pod šifriranjem z javnim ključem in digitalnim potrdilom.
- Brskalnik ustvari ključ za enkripcijo s simetričnim ključem, ga zakodira s strežnikovim javnim ključem in ga pošlje strežniku.
- Strežnik prejet ključ dekodira s privatnim ključem.
- Nadaljnja komunikacija poteka preko enkripcije s simetričnim ključem, ki je veliko hitrejša za šifriranje in dešifriranje podatkov. Istočasno poteka tudi preverjanje o istovetnosti podatkov, da podatki med prenosom slučajno ne bi bili spremenjeni.

SSL certifikat je digitalno potrdilo oziroma elektronski dokument z digitalnim podpisom. Uporabljamo ga pri komunikaciji preko SSL protokola. Vsebuje javni in privatni ključ, ki sta uporabljena za vzpostavitev varne kriptirane spletne povezave. Vsebuje pa tudi podatke o njegovem imetniku in izdajatelju (Presentia, 2010c).

Obstajata dve vrsti SSL certifikatov:

- zaupanja nevreden; je samo podpisan.
- Zaupanja vreden; je podpisan s strani avtoritete. Pri poslovanju, kjer je varnost najpomembnejša, mora biti certifikat podpisan s strani priznanega izdajatelja digitalnih potrdil. Podpis je potrditev, da javni ključ pripada specifičnemu imetniku.

Certifikat SSL lahko kupimo pri operaterju spletišča, za kar potrebujemo:

- ime spletne strani,
- kontaktni e-naslov,
- podatke o podjetju,
- uradni kontaktni e-naslov nosilca domen.

Navadno so v SSL certifikatu naslednji elementi:

- serijska številka,
- oseba, ali podjetje, na katerega se nanaša,
- uporabljen algoritem za kreiranje podpisa,
- podpis podjetja, ki je preverilo in izdalo certifikat,
- datum veljavnosti,
- opis razloga uporabe javnega ključa,
- številka javnega ključa,
- algoritem, ki se uporablja za kriptiranje javnega ključa.

1.2.3 Varnost elektronske pošte

Elektronska pošta (ang. *e-mail*) so sporočila, ki so sestavljena tako, da jih lahko pošiljamo in prejemamo po elektronskih komunikacijskih sistemih. Predstavlja drugo najpogostejšo uporabo interneta (Tschabitscher, 2016).

Namenjena je izmenjavi elektronskih sporočil med dvema ali več naslovniki. Preko nje pa lahko pošiljamo tudi pripete datoteke. Komunikacija je mogoča po celem svetu med posamezniki in podjetji.

Elektronska pošta ima velike prednosti uporabe:

- naslovnika doseže kjerkoli po svetu v zelo kratkem času.
- Pošiljanje je praktično brezplačno, saj ni potrebe po nobeni fizični obliki tiska, ovojnicah in znamkah.
- Omogoča enostavno prilaganje različnih datotek.

- Upravljalniki elektronske pošte nam omogočajo enostavno shranjevanje in arhiviranje vse prispele in oddane pošte.

Elektronska pošta je sestavljena iz:

- elektronskega naslova prejemnika ali več prejemnikov. Ta je sestavljen iz imena prejemnika in ponudnika strežnika. Med njima je znak @ (ang. at);
- naslova, oziroma predmeta sporočila, ki je kratek povzetek sporočila;
- besedila sporočila;
- pripete datoteke.

Prenos elektronske pošte preko interneta poteka po protokolu SMTP (ang. *Simple Mail Transfer Protocol*), ki je preprost protokol za prenos elektronske pošte. Z njimi prenašamo elektronsko pošto med različnimi sistemi, povezanimi s TCP/IP.

SMTP protokol je zapisan v RFC 822, ki je standard računalniškega zapisa in definira strukturo SMTP sporočila. SMTP sporočilo je serija raznoraznih glav naslovov in teles oziroma besedila sporočila, ki je zgrajeno samo iz ASCII znakov (ang. *American Standard Code for Information Interchange*). Priponke v tem standardu niso vključene (Colos, 2016).

RFC 822 standard, ne vsebuje nobenih resnih varnostnih mehanizmov, zato so sporočila, ki niso kriptirana, berljiva vsem, ki lahko posežejo v komunikacijski kanal med pošiljateljem in prejemnikom sporočila.

PGP enkripcija (ang. *Pretty Good Privacy*) je program za kodiranje vsebine datotek, dokumentov, elektronskih sporočil in celih particij na računalniških diskih. Pri kodiranju PGP uporablja kriptografsko metodo javnega in zasebnega ključa z uporabo RSA in IDEA algoritmov, kar pomeni, da imata tako pošiljatelj kot prejemnik vsak svoj par javnih in zasebnih ključev. Javni ključ, kot je že z imena razvidno, objavita, zasebnega pa skrijeta in obdržita zase. Omogoča varno komunikacijo z neznanimi osebami oziroma podjetji brez varnih kanalov potrebnih za izmenjavo ključev (Pretty Good Privacy, 2016).

Kodiranje poteka tako, da pošiljatelj sporočilo zakodira s prejemnikovim javnim ključem in svojim zasebnim ključem. Prejemnik lahko sporočilo dekodira samo s pošiljateljevim javnim ključem in svojim zasebnim ključem. S tem se izognemo potrebi po nekem varnem načinu, preko katerega je potrebno v primeru klasične kriptografije prenesti geslo od pošiljatelja do prejemnika. Ker ni potrebno prenesti gesel in jih tako tudi ni mogoče prestreči, je se tem sistem bistveno cenejši in veliko varnejši.

MIME (ang. *Multipurpose Internet Mail Extension*) oziroma večnamenska razširitev elektronske pošte omogoča razširitev formata elektronske pošte tako, da ta podpira (Presentia, 2008):

- besedila v zakovni kodi, ki ni ASCII (ang. American Standard Code for Information Interchange). ASCII je najbolj pogost tekstovni format uporabljen na računalnikih in spletu;
- priponke, ki ne vsebujejo besedila ;
- telo besedila;
- glavo sporočila, ki ne vsebuje ASCII znake.

Vsaka pošta, ki jo sestavimo v programu, ki podpira MIME, gre čez dva procesa:

- če je sporočilo besedilo v navadni ASCII obliki, ga program pusti v primarni obliki in sporoči naslovniku elektronske pošte, da naj pričakuje le besedilo.
- Če sporočilo vsebuje še kakšno priponko ali besedilo v HTML obliki (ang. Hyper Text Markup Language) oziroma jezik za označevanje nadbesedila, je vsak del pregledan in obravnavan posebej.

Najprej se določi format, da se lahko sporoči prejemniku, kaj naj pričakuje in kaj naj z določenimi podatki stori. Nato se kodira besedilo in vstavi v sporočilo. Če so priložene še priponke, se te opiše oziroma označi, kako naj bodo pri prejemniku dekodirane. Pri prejemniku se proces obrne. Preveri se, če so sporočilu pripete priponke in kako se dekodirajo, kako se dekodira besedilo. Nato prejemnik na podlagi prejetih podatkov in navodil za dekodiranje sestavi enak format sporočila, kot ga je poslal pošiljatelj.

MAC (ang. *Message Authentication Code*) je kodirana avtentikacijska koda. Je simetrični kriptografski ključ, ki zagotavlja pristnost sporočila, da je ta prišel od pošiljatelja in med prenosom ni bil spremenjen. Pripeta je osnovnemu sporočilu (Tutorialspoint, 2016b).

MAC ima dve večji oviri:

- obe stranki morata imeti shranjen isti ključ. To pomeni, da je potrebno pred izmenjavo podatkov preko MAC-a pridobiti, oziroma prenesti ključ obema strankama.
- MAC tehnika je zatajiva, kar pomeni, da lahko ena od strank zanika prejem sporočila.

1.2.4 Varnostni žetoni

Varnostni žetoni (ang. *Security Token*) so namenjeni avtentikaciji pošiljatelja sporočila. Namenjeni so uporabi namesto varnostnega gesla oziroma so podani poleg varnostnega gesla, ki uporabniku omogoča dostop do določene spletne strani (Verdonik, 2005).

Poznamo tri glavne vrste:

- žeton, ki vsebujejo uporabniško ime in geslo (ang. Username Token), omogoča preprosto vključitev uporabniškega imena in gesla v sporočilo. Geslo je lahko prikrito ali neprikrito. Je zelo preprost za uporabnika in če uporabimo še zgoščevalni mehanizem, je ta oblika tudi zelo varna. Problem je, da morata strežnik in odjemalec poznati isto geslo.
- Žeton, ki vsebujejo binarne podatke (ang. Binary Security Token). Z njim lahko v ozadje sporočila vključimo digitalno potrdilo, potrebno za avtentikacijo, digitalne podpise ali biometrične podatke, kot so prstni odtisi.
- Žetonov XML je več vrst. Prikriti elementi so znotraj sporočila v simetričnih in asimetričnih algoritmih

1.2.5 Požarni zid

Požarni zid je najbolj osnovna in razširjena zaščita računalniških sistemov. Je programska ali strojna oprema, ki ločuje odseke omrežja med seboj. Požarni zid praviloma ločuje notranje, krajevno omrežje računalnikov in zunanje, javno omrežje, navadno internet. Pravila, ki jih določimo v požarnem zidu, dovolijo ali onemogočijo komunikacijo med dvema omrežnima točkama oziroma dvema odsekoma omrežij (Mesojedec, 2005).

Funkcije požarnega zidu so:

- omejevanje dostopa prejetih in oddanih paketov podatkov na podlagi protokolov in logičnih vrat, ki jih uporabljajo posamezne spletne storitve;
- prestrezanje vseh poslanih in prejetih podatkov in prepuščanje samo dovoljenim;
- omogoča povezavo po šifriranih poteh, omogoča virtualna privatna omrežja VPN (ang. Virtual Private Network);
- preslikava zasebnih omrežnih naslovov NAT (ang. Network Address Translation), ki omogočajo skupno rabo internetne povezave;
- pregleduje lahko detajle prejetih paketov in identiteto pošiljatelja ter naslovnika;
- omejuje izpostavljenost zasebnega omrežja pred javnim s kontrolnimi točkami.

Glede na sloj protokola, kjer požarni zid opravlja svoje delo, poznamo tri vrste, sodobni požarni zidovi pa so navadno kombinacija vseh:

- paketni filtri (ang. Packet Filter),
- nadomestni strežnik (ang. Proxy Server),
- analiza stanja (ang. Stateful inspection).

Paketni filtri (ang. *Packet Filter*) so zaščita, ki deluje na protokolu povezave. Podatke izmenjujejo v omrežju. Uporabljajo obvladljivo velike pakete podatkov, ki jih drug za

drugim izmenjujejo, dokler ni prenesena vsa vsebina. Paket vsebuje poleg dela celotne vsebine tudi podatke o svojem izvoru in cilju. Paketni filtri na podlagi prebranih podatkov odločajo, ali bodo določen paket sprejeli ali zavrnili.

Učinkovitost paketnega filtra je odvisna od pravil, ki jih predpišemo. To so seznami poskusov, ki jih mora opraviti vsak paket, preden se določi, kaj se bo z njim zgodilo. Običajno postavimo neko temeljno pravilo, ki zavrača vse pakete. Nato pa pravila nadgrajujemo z natančnimi dovoljenji. Tako lažje poskrbimo za varnost, saj določimo samo, kaj je dovoljeno in ne, kaj vse je prepovedano.

Nadomestni strežnik (ang. *Proxy Server*) deluje na višjih nivojih omrežnih protokolov kot paketni filtri. Ne preprečuje prometa le na sloju posameznih paketov, temveč sledi njihovemu zaporedju.

Vsaka povezava ima fazo vzpostavitve. Nadomestni strežnik se ob poskusu povezave postavi v vlogo prejemnika in preveri, če je zaporedje paketov pravilno. Če to potrdi, vzpostavi povezavo med obema stranema. Zaradi učinkovitosti lahko požarni zid po uspešni vzpostavitvi povezave opusti preverjanje protokola in slepo posreduje pakete med obema stranema. To delovanje je hitrejše, a bolj tvegano, zato je pogostejši pristop z stalnim preverjanjem.

Nadomestni strežnik opravlja še eno storitev za večjo varnost krajevnega omrežja, to je, da vzpostavlja povezave v imenu drugih naprav. Tako vse naprave v krajevnem omrežju na zunaj predstavlja pod svojim, zunanjim naslovom IP. Zato uporablja še podrobnejša pravila kot paketni filtri.

Analiza stanja (ang. *Stateful inspection*) je požarni zid, ki odpravlja slabosti nadomestnega strežnika, katerega je nekoliko težko uporabljati. Požarni zid z analizo stanja prometa opravlja vse vloge zaščite kot paketni filtri in nadomestni strežnik. Od nadomestnega strežnika se razlikuje analiza podrobnosti posameznega protokola. Namesto na dejanske protokole se analiza stanja zanaša na posamezne algoritme, ki spremljajo vzorce bitov v paketih. Njihova prednost je, da jih ni potrebno prilagajati vsakemu posameznemu protokolu in so uporabniku nevidni.

1.2.6 Spletni brskalnik

Spletni brskalnik (ang. *Web Browser*) je računalniški program, ki uporabniku omogoča povezavo in uporabo svetovnega spleta-interneta. Omogoča prikazovanje spletnih virov, kot so HTML (ang. *Hyper Text Markup Language*), jezik za označevanje hiper besedil in večpredstavne vsebine, kot so slike in video. Osnovna funkcija spletnega brskalnika je, da uporabniku dostavi in predstavi informacije z interneta (Pečjak, 2005).

Ker so spletni brskalniki direktna povezava računalnikov in njihovih sistemov z internetom, so zaradi tega podvrženi stalnim napadom. Najpogosteje se brskalnike napada da bi:

- prikazovali nezaželene oglase,
- zbirali osebne informacije za namen marketinga in kraje identitete,
- preverjali brane spletne strani,
- vstavljali viruse, trojanske konje, zlonamerne kode in računalniške črve…

Ranljivost lahko zmanjšamo z rednim posodabljanjem in uporabo skupaj z dobro nastavljenim požarnim zidom, ki bo preprečil dostop do zlonamernih strani in opravljal varnostni pregled vseh naloženih datotek.

1.3 Varnostni produkti

Razvijalci programov skrbijo, da so uporabnikom na trgu vedno na voljo najsodobnejši varnostni programi, ki so napisani po varnostnih protokolih. Z njimi se lahko uporabniki z pravilno uporabo zaščitijo pred nevarnostmi spletnega komuniciranja in prenosa podatkov. Mednje prištevamo upravljalnike gesel, protivirusne programe in varnostne pakete.

1.3.1 Upravljalniki gesel

Upravljalnik gesel je program, ki nam pomaga shranjevati in urejati gesla. Navadno shranjuje vsa gesla šifrirano pod določenim skupnim geslom. Uporabniku omogoča vpogled v vsa shranjena gesla na enem mestu. Nekateri upravljalniki gesla shranjujejo na računalnik, drugi pa v oblake. To so internetne baze podatkov, ki so dostopna z vseh lokacij (Vidmar, 2015).

Prednosti upravljalnikov gesel so, da so vsa gesla, ki jih potrebujemo, na enem mestu in da do njih lahko dostopamo, če si zapomnimo le eno geslo. To mora biti zaradi varnosti karseda kompleksno. Uporabljajo zelo varne algoritme, zato v njihove shrambe praktično ni mogoče vdreti. Ker so enostavno vgrajena v programe in brskalnike, znajo gesla tudi sami poiskati in sami vpisati v program ali brskalnik, pri tem pa pazijo, da podatki niso prestreženi.

Največje napake in nevarnost za upravljalnike gesel povzročajo uporabniki sami z:

- enostavnimi gesli, ki so prekratka in se jih zlahka najde v slovarjih. Hkrati uporabljajo enake črke, namesto da bi mešali male in velike ter dodali vmes tudi števila;
- gesli, ki jih shranijo v tiskani obliki;
- se prijavljajo kot administratorji, kjer to ni potrebno;
- uporabo istih gesel na več različnih spletnih straneh;

- delijo gesla z drugimi uporabniki.

1.3.2 Protivirusni programi

Protivirusni programi so računalniški programi, namenjeni zaščiti računalnika pred računalniškimi virusi, črvi, zlonamernimi kodami in trojanskimi konji. Zlonamerne programe poiščejo in odstranijo. Lahko jih uporabljamo za posamezna preverjanja datotek ali pa določimo stalno pripravljenost in sprotno preverjanje prenesenih podatkov. Najdene okužene datoteke se lahko prečisti, če to ni dovolj pa se jih popolnoma odstrani (Martinčič, 2015).

Kljub velikemu razvoju in vlaganju v protivirusne programe moramo poznati določena dejstva:

- noben protivirusni program ni popolnoma zanesljiv.
- Nekateri virusi so sposobni deaktivirati protivirusni program.
- Poznamo programe za domačo in poslovno rabo.
- Različni programi so zaradi svoje zgradbe in delovanja primerni za različne uporabnike.
- Navadno ne delujejo dobro, če delujejo hkrati z drugimi podobnimi programi. To lahko zelo upočasni računalnik.
- Najboljša preventiva je uporaba preverjene programske opreme in brskanje po znanih spletnih straneh.
- Skrbeti moramo za redno osveževanje programa in njegove knjižnice zlonamernih programov.

1.3.3 Varnostni paketi

So tako imenovani skupki programov, ki jih lahko kupimo na trgu in so namenjeni varovanju računalniških sistemov. Paketi se med posameznimi proizvajalci razlikujejo in lahko ponujajo tudi več deset različnih programov. Večini je skupno, da ponuja protivirusne programe in požarni zid. Vsebujejo pa lahko še različne programe, kot so (Robar, 2009):

- protivohunski (ang. Anti-Spyware),
- protireklamni (ang. Anti-Adware),
- protismetni (ang. Anti-Spam),
- programi za starševski nadzor (ang. Parental control),
- program za zaznavanje in odpravo koreninskih kompletov (ang. Anti-Rootkit),
- program za zaznavanje spletnega ribarjenja (ang. Anti-fishing),
- programe za izdelavo varnostnih kopij,
- upravljalniki gesel.

2 DENARNE TRANSAKCIJE

Poleg varnega komuniciranja preko spleta podjetnika verjetno najbolj zanimajo prejeta plačila. Obstaja ogromno možnosti plačevanja, ki pa se največkrat razlikujejo geografsko. Podjetniki imajo omejene možnosti denarnih transakcij glede na njihovo lokacijo. Predstavili bomo v Sloveniji najbolj dostopne in najbolj praktične možnosti plačevanja v spletnih trgovinah, ter kako je poskrbljeno za njihovo varnost (Data, 2016).

2.1 Plačilo po povzetju

Plačilo po povzetju, je tako za kupca in prodajalca ena najenostavnejših možnosti plačevanja blaga, naročenega preko interneta. Je kupcem zelo znana metoda, zato ji tudi zelo zaupajo (Data, 2016).

Prednosti:

- plačilo blaga se opravi v času dostave, kar je podobno klasični trgovini.
- V primeru neplačila se blago vrne prodajalcu.
- Plačilo je možno z gotovino ali s plačilno kartico.
- Plačila potekajo preko dostavne službe.
- Plačila se po pogodbi nakaže direktno na prodajalčev transakcijski račun.
- Za dostavo in plačila skrbi eno podjetje.
- Zmanjša se tveganje goljufije in neplačil.
- Hiter transfer pobranih odkupnin.
- Sledenje plačilne zgodovine preko interneta in sledenje paketov.

Slabosti:

- v primeru neplačila se prodajalcu računa upravljanje s paketom.
- Kupec lahko enostavno zavrne plačilo.
- Zelo omejeno območje delovanja. Večina sveta za slovenske spletne trgovine ni dosegljiva.
- Relativno velika provizija.

2.2 Bančno nakazilo

Bančno nakazilo oziroma plačilo po predračunu je lahko lokalni ali mednarodni prenos sredstev z enega bančnega računa na drugega. Je prodajalcu izredno prijazen način plačevanja, saj so stroški takega plačevanja minimalni, blago pa je plačano pred odpremo.

Prednosti:

- možno je tako lokalno kot mednarodno nakazilo.
- Nakazila se lahko izvajajo v domači valuti.
- Velika transparentnost.
- Blago je plačano pred samo odpremo.

Slabosti:

- plačilo je prejeto relativno počasi: 1-5 delovnih dni, odvisno od države, iz katere se plačilo izvrši.
- Relativno nerodno izpolnjevanje obrazcev v spletnem bančništvu ali v banki.
- Države imajo različne standarde, zato je potrebno preverjanje zahtevanih podatkov.
- Plačila čez vikend so videna in izvedena šele ob naslednjem delovnem dnevu.
- Kupec mora prodajalcu zaupati, da izvede plačilo pred prejetjem blaga.

2.3 Plačilne kartice

Plačilne kartice imenujemo tudi plastični denar. Lastniku omogočajo prenos denarnih sredstev. Njihova uporaba se je začela že leta 1950 v ZDA, nato pa so se pričele uporabljati tudi v Evropi in svetu. Najprej so bile to kartice zaprtega tipa in so se lahko uporabljale le v določenih verigah podjetij, nato pa so se razširile v bančne sisteme (mojdenar, 2016).

V Sloveniji smo jih po malem začeli uporabljati v 60. letih, pravi razmah pa so doživele v zadnjih desetletjih, ko so na trgu začeli delovati tudi domači izdajatelji in ponudniki. Prva plačilna kartica v Sloveniji je bila American Express, ki se je začela uporabljati leta 1968. Danes se v Sloveniji uporablja večji del domačih plačilnih kartic, od tega večina osebnih.

Poznamo več vrst plačilnih kartic, ki jih lahko ločimo po različnih kriterijih: glede na izdajatelja, tip, oziroma čas plačila in kje lahko z njimi plačujemo.

Glede na izdajatelja delimo plačilne kartice na:

- Bančne kartice, ki jih izdajajo banke;
- podjetniške kartice, ki jih izdajajo večja trgovska podjetja;
- partnerske kartice, ki jih izdajajo banke za podjetja;
- licenčne kartice, ki jih izdajajo banke in podjetja s sodelovanju s podjetji iz tujine. V Sloveniji so to npr. kartice Eurocard/Mastercard, Visa, Diners, American Express.

Glede na funkcijo, ki jo plačilne kartice opravljajo, ločimo:

- predplačniške kartice, ki jih vnaprej kupimo, napolnimo in po uporabi lahko tudi zavržemo. To so poleg bančnih kartic tudi razne telefonske kartice, kartice za plačevanje parkirnine, avtobusa…
- Debetne kartice se izda na vezan tekoči račun. Nakup in dvig gotovine se takoj bremeni na tekočem računu. Primer sta BA in Maestro.
- Kreditne kartice oziroma kartice z odloženim plačilom. Nakup in dvig gotovine se bremeni enkrat v mesecu; do takrat kreditira banka. Primer kartic v Sloveniji so Activia, Visa, EC/MC, Diners Club.
- Posojilne kartice, namenjene takojšnjim nakupom in obročnemu odplačevanju. Primer je posojilna Karanta, posojilna Visa.

2.3.1 Debetne kartice

Debetna kartica se izda na podlagi odprtega transakcijskega računa pri banki. Vse opravljene transakcije se takoj bremenijo na transakcijskem računu. Uporabljajo se za dvig gotovine, na bankomatih in v bankah, za nakupe v spletnih trgovinah in za plačevanje preko POS terminalov. POS terminal je tehnologija, ki omogoča avtomatski prenos oziroma izmenjavo podatkov prek terminala, ki je nameščen na nekem prodajnem mestu, do računalnika v banki ob uporabi javnega omrežja. Debetne kartice so postale tako priljubljene, da so skoraj izrinile uporabo čekov in močno zmanjšale uporabo gotovine (The UK Cards Association, 2016; Svetavladar, 2016).

Prednosti debetne kartice:

- večina omogoča uporabo tako v domačih kot tujih trgovinah.
- Omogočajo brezgotovinsko plačevanje in dvig gotovine na bankomatih.
- Omogočajo varno plačevanje, predvsem preko POS terminalov in tudi preko interneta.
- Omogočajo enostaven dostop do bančnega računa.
- Njihova uporaba se navadno ne računa za posamezni nakup in obresti se ne plačujejo. Plačuje se mesečno upravljanje računa.
- V primeru pozitivnega zneska računa banka plačuje minimalne obresti.

Slabosti debetne kartice:

- limit, ki omejuje njihovo uporabo.
- Večina slovenskih kartic ne omogoča plačevanje preko interneta.
- V primeru prekoračitve limita se zaračuna nadomestilo.
- Dvig gotovine z bančnih avtomatov nematične banke se navadno računa.

2.3.2 Predplačniške kartice

Predplačniške kartice so nekakšne debetne kartice, ki niso vezane na določen transakcijski račun uporabnika. Prav tako se uporabljajo za dvig gotovine, na bankomatih in v bankah, za nakupe v spletnih trgovinah in za plačevanje preko POS terminalov. So poenostavljena verzija debetne kartice.

Poznamo več vrst predplačniških kartic. Najpogostejše so darilne kartice, kjer podjetja naložijo določeno vsoto na kartico in se uporabljajo za nakupe v njihovih trgovinah, predplačniške kartice s fiksnim zneskom, na katere ni mogoče ponovno naložiti sredstev, in kartice, na katere lahko večkrat naložimo denarna sredstva (The UK Cards Association, 2016; Svetavladar, 2016).

Prednosti predplačniške kartice:

- večina omogoča uporabo tako v domačih kot tujih trgovinah.
- Omogočajo brezgotovinsko plačevanje in dvig gotovine na bankomatih.
- Omogočajo varno plačevanje predvsem preko POS terminalov in tudi preko interneta.
- Preprečujejo preveliko potrošnjo oziroma kreditiranje, zaradi česar so primerne tudi za otroke.
- Ponujajo večjo varnost na potovanjih, saj jih lahko uporabljamo namesto gotovine.
- Omogočajo plačevanje s karticami ljudem, ki zaradi različnih razlogov ne morejo priti do debetne ali kreditne kartice.
- Velikokrat ponujajo možnost bremenitve enega račun z več karticami.
- V primeru kraje storilec nima dostopa do našega bančnega računa.

Slabosti predplačniške kartice:

- višji stroški vodenja in uporabe.
- Limit, ki omejuje njihovo uporabo.
- Večina slovenskih kartic ne omogoča plačevanje preko interneta.
- Dvig gotovine z bančnih avtomatov nematične banke se navadno računa.
- Obresti na naložen denar se ne izplačuje.
- Nekatere kartice ponujajo nižjo zaščito kot debetne in kreditne kartice.
- Nekatere kartice imajo s strani izdajatelja postavljene dodatne omejitve uporabe.
- Velikokrat imajo postavljeno minimalno in maksimalno višino, ki jo lahko naložimo na kartico, maksimalno višino, ki je lahko na kartici, maksimalno višino, ki jo lahko dnevno dvignemo, ali minimalni znesek, ki ga lahko plačamo.
- Ker kartice niso vezane na določeno ime, izdajatelji ne ponujajo nobenega zavarovanja v primeru goljufije.

2.3.3 Kreditne kartice

Kreditna kartica je kartica z odloženim plačilom in je namenjena tistim, ki se nočejo obremenjevati s trenutnim stanjem na računu. Uporabniku omogoča nakup izdelkov ali plačilo storitev takoj, poravna pa vse skupaj enkrat na mesec, na dan, ki si ga sam izbere. Možen je tudi odlog plačila oziroma banka določi minimalno vsoto, ki jo je potrebno mesečno plačevati. Preden uporabnik poplača nakupe, plačilo in kritje plačila prevzame banka. Kreditno kartico lahko dobi polnoletna oseba, ki ima pri banki izdajateljici odprt transakcijski račun. Banka zaračuna letno članarino in po dogovoru določi mesečni limit (The UK Cards Association, 2016; Svetavladar, 2016).

Kreditne kartice se ločuje predvsem glede na to, kakšno plačilno sposobnost ponujajo. Poleg osnovne, banke ponujajo še razne prestižne kartice, kot so platinaste, zlate in podobno. Poleg višje plačilne sposobnosti te za sabo potegnejo tudi večje stroške, hkrati pa banka močno nadzira in preverja, kakšno kreditno kartico nudi.

Prednosti kreditne kartice:

- omogočajo nakupe z odloženim plačilom, tako imenovano kratkoročno kreditiranje.
- Večina omogoča uporabo tako v domačih kot tujih trgovinah.
- Omogočajo brezgotovinsko plačevanje in dvig gotovine na bankomatih.
- Omogočajo varno plačevanje predvsem preko POS terminalov in tudi preko interneta.
- Omogočajo nakupe v spletnih trgovinah.
- So v večini zavarovane proti goljufiji.
- Ponujajo dodatno zavarovanje pri plačilu v spletnih trgovinah.
- Omogočajo enostaven dostop do bančnega računa preko telefona ali interneta.

Slabosti kreditne kartice:

- nepremišljeno ravnanje lahko pripelje do nepričakovanega zadolževanja.
- Večji stroški, če zamujamo s plačili.
- V primeru neplačevanja lahko pridemo na tako imenovano črno listo, kar nam oteži in podraži pridobitev nove kreditne kartice.
- Če jo uporabljamo kot možnost kreditiranja, nas to stane več kot običajni krediti.
- Ob večjem številu kartic lahko izgubimo nadzor nad svojimi financami.

2.3.4 Posojilne kartice

Posojilne kartice omogočajo nakup z odlogom v okviru odobrenega posojila. Razlika med kreditno in posojilno kartico je, da se pri slednji vsak mesec samodejno poravna le del plačilnega prometa, ki je bil opravljen z njo. Za še neplačani dolg pa banka zaračuna obresti. Višina odobrenega posojila je odvisna od finančnega stanja (Krisper, 2016).

Prednosti posojilne kartice:

- omogočajo nakupe z odloženim plačilom.
- Omogočajo hiter dostop do kredita.
- Omogočajo brezgotovinsko plačevanje in dvig gotovine na bankomatih.
- Omogočajo varno plačevanje predvsem preko POS terminalov in tudi preko interneta.
- Omogočajo nakupe v spletnih trgovinah.
- So večinoma zavarovane proti goljufiji.

Slabosti posojilne kartice:

- je manj primerna za dvigovanje gotovine, saj banka zaračuna provizijo v odstotkih dvignjenega zneska.
- Večinoma so višji stroški članarine kot pri kreditnih karticah.
- Večja verjetnost izgube nadzora nad zadolževanjem.

2.3.5 Varnost plačilnih kartic

Varnost plačilnih kartic se zagotavlja s fizičnim varovanjem in varovanjem številke kartice. Zelo pomembno je, komu se zaupa številka kartice. Nekatere banke zahtevajo od uporabnika tudi PIN številko (kodno varovana kartica).

Poslovanje s plačilnimi karticami poteka po standardu PCI DSS (ang. *Payment Card Industry Security Standard Council*), ki bankam veleva, naj od svojih trgovcev zahtevajo rokovanje s plačilnimi karticami po standardu, ki veleva (Rouse, 2009):

- namestitev in vzdrževanje požarnega zidu za zaščito podatkov imetnika kartice;
- neuporabo privzetih nastavitev sistemov, gesel in drugih varnostnih parametrov;
- zaščito shranjenih podatkov imetnika kartice;
- prenosi podatkov imetnika kartice po odprtih javnih omrežjih morajo biti kriptirani;
- zahtevana je uporaba in redno posodabljanje protivirusne programske opreme;
- potrebno je razvijati in vzdrževati varne sisteme;
- omejiti dostop do podatkov imetnikov kartic, na minimum;
- določiti enolično identifikacijsko številko za vsako posamezno osebo z dostopom do računalnika;
- potrebno je fizično omejevanje dostopa do podatkov imetnikov kartic;
- redno testiranje varnostnih sistemov in procesov.

Kartice so dodatno zaščitene tudi z vodnimi znamenji in hologrami. Za večjo zaščito so banke uvedle tako imenovane pametne kartice, ki so izdelane po EMV standardu. EMV je odprt industrijski standard, ki zagotavlja povezljivost kartic in naprav. Zagotavlja, da so vse kartice izdelane po istem standardu ne glede na to, kdo je izdajatelj in kakšna banka

stoji v ozadju. Za transakcije je potrebna pametna kartica z vgrajenim vezjem ali čipom in naprava ki jo podpira. Večjo varnost zagotavlja s preverjanjem vgrajenega PIN-a. EMV standardi so vstopili v dokončno veljavo 1. 1. 2005 (Activa, 2016).

Poleg zaščite plačilnih kartic, za katero skrbijo banke in podjetja, morajo svoje opraviti tudi uporabniki sami ob tem, da se držijo določenih pravil (Združenje bank Slovenije, 2016):

- veljavna je le podpisana kartica, zato jo je potrebno ob prejemu nemudoma podpisati.
- S kartico je potrebno ravnati skrbno in je ne izpustiti izpred oči.
- Osebno številko (PIN) za kartico si je treba zapomniti in ne shranjevati.
- Številka kartice in še posebej njeni podatki, PIN, datum veljavnosti, CVC2 koda (trimestna številka zapisana na podpisanem traku na hrbtni strani krtice) so tajni.
- Pri nakupih je potrebno preveriti znesek na izpisku in ga nato uničiti, da ne bi morebiti izgubili zaupnih podatkov.
- Preko interneta se plačuje in daje številko kartice le zaupanja vrednim podjetjem.
- Izgubo ali krajo je potrebno nemudoma prijaviti.

2.4 PayPal

Za slovenska podjetja s spletno trgovino je poleg plačil po povzetju, bančnih nakazil in raznih plačilnih kartic najbolj enostaven in priljubljen način prejemanja plačil sistem PayPal, ki ga je leta 1998 v Kaliforniji uvedlo podjetje Paypal Holding inc. Skrbi za prenos elektronskih plačil med njenimi strankami. Svojim strankam dovoli odpiranje računov na lastnih spletnih straneh, računi pa so bremenjeni preko njihovih plačilnih kartic. Njegovo poslovanje temelji na že obstoječem internetnem bančnem poslovanju, ki ga nadgradi z napredno tehnologijo proti prevaram in s tem še dodatno poskrbi za varnost transakcij (Skinner, 2007).

2.4.1 Delovanje PayPal

Paypal deluje na podlagi kriptiranih programov, ki omogočajo varne transakcije. Skrbi za varne transakcije med posamezniki ali podjetji in deluje kot posrednik, ki prenaša finančna sredstva iz osebnih računov in kreditnih kartic neposredno drugim posameznikom ali podjetjem. Za osnovno prijavo in prejetje sredstev je potreben le naslov elektronske pošte (Grabianowski & Crawford, 2005).

Prednosti:

- enostavna uporaba. Transakcije se lahko opravi samo z vpisanim e-mail naslovom brez dolgotrajnega pisanja podatkov o kreditni kartici.

- Osebne podatke in podatke o kreditni kartici, se vpiše samo enkrat in ne ob vsaki transakciji.
- Osebne podatke in podatke o kreditni kartici pozna in shranjuje samo PayPal in ne vse stranke udeležene pri transakcijah.
- Močna podprtost proti prevaram in krajam.
- Plačila se izvedejo v trenutku potrditve naročila.
- Storitve PayPal so globalno prisotne, kar omogoča enostaven nakup in prodajo po celem svetu.
- Brezplačno odprtje osnovnega računa.
- Kupci ne plačujejo provizije.
- Spletnim trgovinam omogoča hitro in enostavno vpetje PayPal programa v spletno trgovino.
- Spletnim trgovinam omogoča cenejše in zelo enostavno brezgotovinsko poslovanje.
- Spletne trgovine, ki podpirajo PayPal plačila, privlačijo večje število kupcev z različnih koncev sveta.

Slabosti:

- deluje kot banka, hkrati pa ni reguliran kot banka in mu ni potrebno delovati po mednarodno sprejetih bančnih standardih.
- Obresti iz denarja na računih pobere PayPal in ne njihovi uporabniki.
- Kompliciranо preverjanje istovetnosti uporabnikov.
- Zamrzovanje uporabniških računov in njihova kompliciranа ponovna uporaba na podlagi dolge verifikacije.
- Uporabniki pogosto ne razumejo poslovanja in pričakujejo, da bodo v primeru goljufije enostavno dobili svoj denar nazaj.
- Uporabniki morajo v primeru goljufije skozi dolg in kompliciran postopek.
- Vloga tožb v postopku prijave goljufije že ob zelo nizkih zneskih.
- Zelo striktna politika zapiranja računov uporabnikom, če za njih obstaja sum terorizma, kar prizadene ogromno nedolžnih ljudi in jim tako prepreči dostop do svojega zakonitega premoženja.
- Za vzpostavitev PayPal računa z vsemi funkcijami je potrebna kreditna kartica ali transakcijski račun.
- Večje omejevanje prodajalcev po geografskem izvoru.

Uporabnik se mora za uporabo PayPal uslug prijaviti oziroma registrirati preko njihove spletne strani, kjer mora posredovati določene informacije. Ker PayPal deluje kot posrednik med bankami kupca in prodajalca, je potrebno vpisati podatke o kreditni kartici ali transakcijskem računu, kontaktne podatke, naslov elektronske pošte in osebno geslo.

Možna je registracija različnih računov (PayPal, 2016):

- osebni (ang. Personal Account), namenjen posameznikom, ki kupujejo preko spleta. Omogoča prenos denarja, prejemanje in nakazila z uporabo elektronskega naslova. Nakazila na osebni račun se lahko izvede preko kreditne ali debetne kartice; zaradi višje provizije pri prejemanju denarja za poslovanje niso primerni.
- Zahtevnejši uporabniki (ang. Premier Account), namenjen posameznikom, ki veliko kupujejo in prodajajo preko spleta, a nimajo registriranega podjetja. Nakazila se lahko izvede preko kreditne ali debetne kartice.
- Poslovni (ang. Business Account) je enak računu za zahtevnejše uporabnike, izdelan pa je za uporabnike, ki želijo poslovati pod imenom podjetja ali organizacije. Poslovni račun mora biti odobren s strani podjetja ali organizacije, za katero se ta račun odpira. Prednost tega računa je, da ga lahko uporablja več uporabnikov, katerim je mogoče omejiti pravice glede na funkcijo, ki jo imajo v podjetju ali organizaciji.

2.4.2 Varnost PayPal-a

PayPal je svoje delovanje posvetil predvsem varnosti. Zaradi svojega stremenja k varnosti in relativno nizke cene uporabe je predvsem primeren za posameznike in manjša podjetja, katerim ni potrebno investirati v drage varne sisteme za prenos denarja. Poleg tehničnega varovanja ponuja tudi zavarovanje proti goljufiji, kjer pa so zavarovani predvsem kupci.
Za varno komunikacijo in zaščito informacij, ki potekajo preko javnega interneta, uporablja tehnologijo SSL. Prenos podatkov se šifrira po najnovejšem protokolu SSL SHA-256 z 2048-bitno enkripcijo (PayPal, 2016b).

3 VARNOST NA PRIMERU SPLETNE TRGOVINE SKYGURU

Skyguru je majhna spletna trgovina, ki ima registrirano domeno in je na spletu predstavljena pod naslovom www.skyguru.eu. Izdelana je v HTML (ang. *Hyper Text Markup Language*) jeziku, kar nam omogoča prikazovanje teksta, slik in različnih povezav na druge spletne strani. Omogoča, da obiskovalec s preprostim klikom na miško pregleduje besedilo, odpira slike in video, ter plačuje preko vgrajene povezave po PayPal-u. Uporaba vseh teh funkcij je mogoča vsem uporabnikom s sodobnim spletnim brskalnikom, ki prepozna obliko html.

Spletna stran je postavljena na lastnem strežniku, ki je na sedežu podjetja in je tako poskrbljeno za njegovo fizično varovanje in s tem varovanje podatkov. Za tehnično varovanje pa skrbita programska oprema in router. Router podjetja Iskratel Innbox F60 je na splet povezan preko optičnega omrežja in onemogoča nepooblaščen zunanji dostop. Za to je poskrbljeno z strogo nastavljenim požarnim zidom. Vse nastavitve strežnika, pregled, posodobitve spletne trgovine in shranjenih podatkov na strežniku potekajo po krajevnem LAN (ang. *Local Area Netvork)* omrežju. S tem smo se še dodatno zavarovali pred napadi preko javnega omrežja – interneta.

Spletno stran se pregleduje in dodeluje na osebnem računalniku, ki je na internet povezan preko routerja in deluje na operacijskem sistemu Windows 10. Za varnost poleg požarnega zidu na routerju, skrbi tudi vgrajeni Windows 10 protivirusni sistem. Ta skrbi za sprotno pregledovanje vseh prenesenih podatkov, hkrati pa izvaja tudi redni sistematski pregled operacijskega sistema. To mu omogoča ažurno posodobljena knjižnica računalniških virusov, zlonamernih kod in trojanskih konjev.

Za komunikacijo s kupci in poslovnimi partnerji je poskrbljeno z odjemalcem pošte Mozilla Thunderbird, ki z vgrajenimi varnostnimi mehanizmi skrbi za varen pretok podatkov. Prav tako je zaščiten s požarnim zidom in protivirusnim sistemom.
Omogočamo plačilo po povzetju, katerega uporabljajo kupci iz Slovenije. Za nas pa ga po pogodbi izvaja Pošta Slovenije, ki skrbi tudi za prevzem in dostavo pošiljk. Transakcije se opravlja enkrat mesečno. Prav tako skrbijo za dostavo izdelkov za kupce ki izberejo možnost plačila z bančnim nakazilom.

Nakup preko PayPal-a je najpogostejša izbira kupcev v spletni trgovini SkyGuru. Omogoča plačevanje preko PayPal računov in s kreditnimi karticami. To smo omogočili z umestitvijo PayPal gumba v html besedilo. Ta skrbi, da komunikacija s kupcem poteka po SSL šifriranem protokolu z 2048-bitno enkripcijo in s tem zagotavlja varno povezavo in varnost podatkov. Kupec se lahko zanese, da so njegovi podatki varni, čeprav prvič kupuje v naši trgovini in nas ne pozna, ker ve, da v ozadju stoji ugledno podjetje, kot je PayPal. PayPal s svojo tehnologijo skrbi, da se plačila kupcev opravljajo preko varne povezave, da so njihovi podatki tajni in da jih naše podjetje ne more videti ter morebiti zlorabiti. Nam pa poenostavi poslovanje, saj nam ni potrebno skrbeti za varne šifrirane povezave in varno shranjevanje zaupnih osebnih podatkov vseh kupcev ter graditi na težko pridobljenem zaupanju kupcev.

Vse to nam je omogočila umestitev PayPal povezave na spletno trgovino in odprtje PayPal računa. Pri registraciji smo izbrali poslovni račun in vpisali vse podatke o podjetju, ime, naslov, s čim se ukvarjamo, uporabniško ime, geslo itd. Po preverjanju pa še vse podatke o kreditni kartici. Po že začetnem poslovanju in prejetju nakazil v vrednosti več kot 1.800 evrov se je PayPal izkazal z njihovo strogo politiko varovanja in preverjanja uporabnikov. Preveriti so želeli našo istovetnost, zato so zahtevali tudi davčno številko, izpis iz sodnega registra in položnico za elektriko, s čimer so si zagotovili, da smo fizično podjetje in ne neka fiktivna organizacija.

V prihodnosti nameravamo varnost spletne trgovine povečati še s pridobitvijo SSL certifikata. Z njim bodo naši kupci, dobili še večje zaupanje in večjo varnost komunikacije. Trenutno je pod zaščito SSL protokola le del strani, ki je namenjena plačilu preko PayPal-a, za kar skrbi njihov certifikat. S pridobitvijo lastnega certifikata pa bomo poskrbeli, da bo celotna spletna trgovina zaščitena z SSL protokolom. SSL nam ponujajo številna slovenska

podjetja, ki nam omogočajo različne stopnje certifikata, s 40- do 256-bitno enkripcijo, različno stopnjo preverjanja in različno možnostjo uporabljanja poddomen.

SKLEP

V zaključku strokovne naloge lahko ugotovim, da je trženje preko spleta prišlo praktično v vse oblike poslovanja, zato se ga ne smemo bati, ampak moramo sprejeti njegove prednosti in poznati slabosti. Skoraj vsako poslovanje je povezano s spletom, zato bi morali vsi poznati vsaj osnovne tehnične zahteve in možnosti. Spletno poslovanje je lahko zelo preprosto ali zelo kompleksno; le če je podprto z znanjem in razumevanjem, je tudi varno. To lahko razumemo kot preprosto dopisovanje preko elektronske pošte ali kompleksno plačevanje preko lastnih programskih in varnostnih rešitev.

V nalogi sem predstavil, da se pri spletnem poslovanju podatki prenašajo preko javnega interneta in so zato zelo ogroženi z različnimi vdori, okužbami, spletnim ribarjenjem, napadi z zavračanjem storitev in ranljivostjo aplikacij. Te nevarnosti rešujemo z uvedbo varnostnih produktov, kot so protivirusni programi, upravljalniki gesel in varnostni paketi. Varnostni produkti delujejo na podlagi protokolov, kot so omrežna varnostna plast, SSL in TLS enkripcija, varnostni žetoni in požarni zidovi. Poleg varnostnih težav, prenosa podatkov in njihovih rešitev sem predstavil tudi denarne transakcije, ki se jih lahko poslužujejo slovenski podjetniki s spletnimi trgovinami. Trgujejo lahko z uporabo plačil po povzetju, bančnimi nakazili, plačilnimi karticami in sistemom PayPal. Prikazal sem, da je spletna trgovina Skyguru varovana z routerjem in požarnim zidom. Dodatno jo varuje protivirusni program. Sprejema različna plačila. Plačilo po povzetju, bančno nakazilo, plačilne kartice, najpogosteje pa uporabljajo sistem PayPal. Sistem plačila PayPal ji omogoča varno kriptirano komunikacijo s kupci. Predstavil sem, da je možna izboljšava z uvedbo SSL certifikata, oziroma digitalnega potrdila, kar bo omogočilo, da bo vsa komunikacija na spletni strani www.skyguru.eu kriptirana po protokolu SSL. Poleg izboljšave bo potrebno skrbeti tudi za pravilno nastavljen požarni zid in redno posodabljanje protivirusnega programa, operacijskega sistema in vseh programov, potrebnih za poslovanje.

S tem sem prikazal, da se lahko vsi podjetniki brez strahu lotijo postavitve spletne trgovine in da lahko za varno poslovanje dobro poskrbijo z uveljavljenimi varnostnimi produkti, ki so na trgu. Potrebno je le osnovno znanje in pravilna uporaba vseh varnostnih produktov.

LITERATURA IN VIRI

1. Neoserv. (b.l.a). *Kako spletno stran obvarovati pred vdori in virusi?*. Najdeno 15.julija.2016 na spletnem naslovu https://www.neoserv.si/podpora/kako-spletno-stran-obvarovati-pred-vdori
2. Neoserv. (b.l.b). *Moja spletna stran je bila napadena/okužena?*. Najdeno 15.julija.2016 na spletnem naslovu https://www.neoserv.si/podpora/moja-stran-je-bila-napadena
3. Man Young Rhee. (2003). *Internet Security, Cryptographic Principles, Algorithms and Protocols*. West Sussex, England: John Wiley & Slon Ltd
4. Si-Cert. (b.l). *Varnostne grožnje*. Najdeno 15.julija.2016 na spletnem naslovu https://www.cert.si/si/varnostne-groznje/
5. MNZ, Policija. (2006, september). *Varni na Internetu.* MNZ RS, Policija, Simpro d.o.o. Najdeno 15.julija.2016 na spletnem naslovu http://www.policija.si/images/stories/Publikacije/PDF/varniNaInternetu.pdf
6. Varni na internetu. (2013a). *Računalniški virusi od a od ž.* Zadrga. Najdeno 30.julija.2016 na spletnem naslovu https://www.varninainternetu.si/2016/racunalniski-virusi-od-a-do-z/
7. Varni na internetu. (2013b). *Vrste zlonamernih programov.* Zadrga. Najdeno 30.julija.2016 na spletnem naslovu https://www.varninainternetu.si/2016/racunalniski-virusi-od-a-do-z/
8. Rouse, M. (2009, oktober). *Denial of service (Dos).* Techtarget. Najdeno 28.julija.2016 na spletnem naslovu http://searchsoftwarequality.techtarget.com/definition/denial-of-service
9. Causey, B. (2016, maj). *How to resolve Web Application security vulnerabilities.* Techtarget. Najdeno 27.julija.2016 na spletnem naslovu http://searchsecurity.techtarget.com/tip/How-to-resolve-Web-application-security-vulnerabilities
10. Tutorialspoint. (2016). *Network Security-Network Layer*. Najdeno 2.avgusta.2016 na spletnem naslovu https://www.tutorialspoint.com/network_security/network_security_layer.htm
11. Presentia. (2010, 4.maj.a). *Kako poteka SSL komunikacija?*. Najdeno 2.avgusta.2016 na spletnem naslovu http://www.presentia.si/baza-znanja-helpdesk/2010/kako-poteka-ssl-komunikacija/
12. Presentia. (2010, 4.maj.b). *Kaj je SSL?*. Najdeno 2.avgusta.2016 na spletnem naslovu http://www.presentia.si/baza-znanja-helpdesk/2010/kaj-je-ssl/
13. Presentia. (2010, 4.maj.c). *Kaj je SSL certifikat?*. Najdeno 2.avgusta.2016 na spletnem naslovu http://www.presentia.si/baza-znanja-helpdesk/2010/kaj-je-ssl-certifikat/
14. Transport Layer Security. (b.l). V *Wikipedija*. Najdeno 29.junija.2016 na spletnem naslovu https://en.wikipedia.org/wiki/Transport_Layer_Security
15. Verdonik, I. (2005, 30.marec). *Varne spletne storitve.* Monitor. Najdeno 29.junija.2016 na spletnem naslovu http://www.monitor.si/clanek/varne-spletne-storitve/121447/?xURL=301

16. Tschabitscher, H. (2016, 26.avgust). *What Email is and How it Works.* Abouttech. Najdeno 27.junija.2016 na spletnem naslovu http://email.about.com/cs/beginningemail/a/email_basics.htm
17. Colos. (b.l). *Simple Mail Transfer Protocol*. Najdeno 26.junija.2016 na spletnem naslovu http://colos.fri.uni-lj.si/eri/RAC_SISTEMI_OMREZJA/html/Aplikacijska_plast/smtp.html
18. Pretty Good Privacy. (b.l). V *Wikipedija*. Najdeno 29.junija.2016 na spletnem naslovu https://sl.wikipedia.org/wiki/Pretty_Good_Privacy
19. Presentia. (2008, 11.september). *Kaj je MIME?*. Najdeno 26.junija.2016 na spletnem naslovu http://www.presentia.si/baza-znanja-helpdesk/2008/kaj-je-mime/
20. Message authentication code. (b.l). V *Wikipedija*. Najdeno 29.junija.2016 na spletnem naslovu https://en.wikipedia.org/wiki/Message_authentication_code
21. Tutorialspoint. (2016b). *Message Authentication.* Najdeno 2.avgusta.2016 na spletnem naslovu http://www.tutorialspoint.com/cryptography/message_authentication.htm
22. Mesojedec, U. (2005, 13.november). *Požarni zidovi*. Monitor. Najdeno 26.junija.2016 na spletnem naslovu http://www.monitor.si/clanek/pozarni-zidovi2/121903/
23. Pečjak, J. (2005, 19.april). *Spletni brskalniki*. Monitor. Najdeno 26.junija.2016 na spletnem naslovu http://www.monitor.si/clanek/spletni-brskalniki/121516/?xURL=301
24. Vidmar, D. (2015, 30.junij). *Z geslom varovana gesla*. Monitor. Najdeno 26.junija.2016 na spletnem naslovu http://www.monitor.si/clanek/z-geslom-varovana-gesla/123746/
25. Martinčič, B. (2015, 25.avgust). *Zastonj ni slabo*. Monitor. Najdeno 25.junija.2016 na spletnem naslovu http://www.monitor.si/clanek/zastonj-ni-slabo/167579/
26. Robar, V. (2009, 31.marec). *Spletni varnostniki*. Monitor. Najdeno 26.junija.2016 na spletnem naslovu http://www.monitor.si/clanek/spletni-varnostniki2/123576/?xURL=301
27. Data. (2016). *Metode plačevanja po spletu*. Najdeno 15.junija.2016 na spletnem naslovu http://data.si/blog/2014/07/21/metode-placevanja-na-spletu-1-del-placilo-po-povzetju-po-predracunu-ter-s-placilno-kartico/
28. The UK Cards Association. (b.l.). *The right payment card for you.* Najdeno 15.junija.2016 na spletnem naslovu http://www.theukcardsassociation.org.uk/individual/right_card.asp
29. Mojdenar. (b.l.). *Plačilne kartice*. Najdeno 15.junija.2016 na spletnem naslovu http://www.mojdenar.com/BANKE/plac_kart_splosno.asp
30. Svetavladar. (b.l). *Vrste bančnih kartic*. Najdeno 15.junija.2016 na spletnem naslovu http://www.svetavladar.si/faks/clanek?aid=192
31. Krisper, B. (b.l). *Posojilne kartice.* Zveza potrošnikov Slovenije. Najdeno 15.junija.2016 na spletnem naslovu https://www.zps.si/index.php/osebne-finance-sp-1406526635/osebni-rauni/5910-posojilne-kartice
32. Activa. (2007, 15.januar). *MasterCard Europe prvi v Evropi izdal socialno pametno kartico, ki izpolnjuje zahteve EMV standarda*. Najdeno 16.junija.2016 na spletnem naslovu http://www.activa.si/novica.asp?ID=59

33. Rouse, M. (2009, maj). *PCI DSS.* Techtarget. Najdeno 15.junija.2016 na spletnem naslovu http://searchfinancialsecurity.techtarget.com/definition/PCI-DSS-Payment-Card-Industry-Data-Security-Standard
34. Združenje bank Slovenije. (b.l). *Kaj je dobro vedeti za varno uporabo bančnih-plačilnih kartic?* Najdeno 16.junija.2016 na spletne naslovu http://portaladmin.unicreditbank.si/Dokumenti/Prebivalstvo/Kartice/Nasveti_ZBS.pdf
35. Skinner, C. (2007, 11.april). Celebrating PayPal's Centenary. Finextra. Najdeno 2.septembra.2016 na spletnem naslovu https://www.finextra.com/resources/feature.aspx?featureid=890
36. Grabianowski E. & Crawford S. (2005, 13.december). *How PayPal Works*. Howstufworks. Najdeno 2.septembra.2016 na spletnem naslovu http://money.howstuffworks.com/paypal.htm
37. PayPal. (b.l.). *Account Types*. Najdeno 2.septembra.2016 na spletnem naslovu https://www.paypal.com/selfhelp/topic/ACCOUNT_TYPES_CA
38. PayPal. (b.l.). *SSL Certificate Upgrade Microsite.* Najdeno 2.septembra.2016 na spletnem naslovu https://www.paypal-knowledge.com/infocenter/index?page=content&widgetview=true&id=FAQ1766&viewlocale=en_US