Elektronsko poslovanje

Problemi zastite i sigurnosti

(prvi dio)

c) **Gubljenje poslova zbog nedostupnosti servisa** – Elektronski servisi mogu biti nedostupni u dužem vremenskom periodu ili u periodu značajnom za obavljanje konkretnog posla, zbog napada na sistem od strane zlonamernih osoba ili zbog slučajnih otkaza sistema. Posledice takvih događaja (finansijske prirode ili druge vrste) mogu biti katastrofalne za jedno preduzeće.

d) **Neovlašćena upotreba resursa** – Napadač koji ne pripada organizaciji koju napada može neovlašćeno pristupiti nekim resursima njenog računarskog sistema i upotrijebiti ih radi pribavljanja imovinske koristi. Tipičan primjer resursa osjetljivog na takvu vrstu napada je telekomunikacioni servis. U opštem slučaju, "hakeri" koriste računar kome su neovlašćeno pristupili kako bi napali ostale računare u mreži.

e) **Gubljenje poslovnog ugleda i poverenja klijenata** – Preduzeće može pretrpjeti značajne gubitke zbog lošeg iskustva svojih klijenata ili zbog negativnog publiciteta koji mogu biti posledica napada na njegov servis elektronske trgovine, ili ponašanja zlonamjerne osobe koja se predstavlja kao pripadnik tog preduzeća.

f) **Troškovi izazvani neizvjesnim uslovima poslovanja** – Česti prekidi funkcionisanja servisa, izazvani napadima spolja ili iznutra, greškama i sl. mogu paralisati izvršenje poslovnih transakcija u značajnom vremenskom periodu. Na primjer, potvrde transakcija koje ne mogu da se prenesu komunikacionim kanalima, transakcije koje mogu biti blokirane od strane trećih lica itd. Finansijski gubici koje ovakvi uslovi poslovanja mogu izazvati mogu biti značajni.

Zbog navedenih problema, potrošači koji koriste takve servise elektronske trgovine mogu pretrpjeti direktne ili indirektne finansijske gubitke.

- Rizici koje sa sobom nosi upotreba elektronske trgovine mogu se izbjeći upotrebom odgovarajućih mjera bezbjednosti
- mjere mogu biti tehnološke i pravne

Osnovni ciljevi mjera bezbjednosti u informacionim sistemima su:

a) **Povjerljivost** – obezbjeđuje nedostupnost informacija neovlašćenim licima.

b) **Integritet** – obezbjeđuje konzistentnost podataka, sprečavajući neovlašćeno generisanje, promjenu i uništenje podataka.

c) **Dostupnost** – obezbjeđuje da ovlašćeni korisnici uvijek mogu da koriste servise i da pristupe informacijama.

d) **Upotreba sistema isključivo od strane ovlašćenih korisnika** – obezbjeđuje da se resursi sistema ne mogu koristiti od strane neovlašćenih osoba niti na neovlašćen način.

Glavne naučne discipline čiji rezultati se koriste da bi se ostvarili pomenuti ciljevi su nauka o bezbjednosti komunikacija i nauka o bezbjednosti u računarima

- **Bezbjednost komunikacija** označava zaštitu informacija u toku prenosa iz jednog sistema u drugi
- **Bezbjednost u računarima** označava zaštitu informacija unutar računara ili sistema – ona obuhvata bezbjednost operativnog sistema i softvera za manipulaciju bazama podataka

Potencijalne prijetnje jednom informacionom sistemu koji sadrži podsistem za elektronsku trgovinu su:

a) **Infiltracija u sistem** – Neovlašćena osoba pristupa sistemu i u stanju je da modifikuje datoteke, otkriva povjerljive informacije i koristi resurse sistema na nelegitiman način. U opštem slučaju, infiltracija se realizuje tako što se napadač predstavlja kao ovlašćeni korisnik ili korišćenjem slabosti sistema (npr. mogućnost izbjegavanja provjera identiteta i sl.). Informaciju neophodnu za infiltraciju, napadač dobija koristeći neku drugu vrstu napada. Primjeri takvih napada su "dumpster diving attack", kod koga napadač dobija potrebnu informaciju pretražujući korpu za otpatke svoje žrtve, i "socijalni inženjering" kod koga napadač dobija neophodnu informaciju primoravajući na neki način (ucjena, prijetnja i sl.) svoju žrtvu da mu je da.

b) **Prekoračenje ovlašćenja** – Lice ovlašćeno za korišćenje sistema koristi ga na neovlašćeni način. To je tip prijetnje koju ostvaruju kako napadači iznutra ("insiders") tako i napadači spolja. Napadači iznutra mogu da zloupotrebljavaju sistem radi sticanja beneficija. Napadači spolja mogu da se infiltriraju u sistem preko računa sa manjim ovlašćenjima i nastaviti sa infiltracijom u sistem koristeći takav pristup radi neovlašćenog proširenja korisničkih prava.

c) **Suplantacija** – Obično poslije uspješno izvršene infiltracije u sistem, napadač ostavlja u njemu neki program koji će mu omogućiti da olakša napade u budućnosti. Jedna od vrsta suplantacije je upotreba "trojanskog konja" – to je softver koji se korisniku predstavlja kao normalan, ali koji prilikom izvršenja otkriva povjerljive informacije napadaču. Na primer, tekst procesor može da kopira sve što ovlašćeni korisnik unese u jednu tajnu datoteku kojoj može da pristupi napadač.

d) Prisluškivanje – Napadač može da pristupi povjerljivim informacijama (npr. lozinci za pristup sistemu) prostim prisluškivanjem protoka informacija u komunikacionoj mreži. Informacija dobijena na ovaj način može se iskoristiti radi olakšavanja drugih vrsta napada.

e) Promjena podataka na komunikacionoj liniji – Napadač može da promijeni informaciju koja se prenosi kroz komunikacionu mrežu. Na primer, on može namjerno da mijenja podatke finansijske prirode za vreme njihovog prenošenja kroz komunikacioni kanal, ili da se predstavi kao ovlašćeni server koji od ovlašćenog korisnika zahtijeva povjerljivu informaciju.

f) **Odbijanje servisa** – Zbog čestih zahtjeva za izvršenje složenih zadataka izdatih od strane neovlašćenih korisnika sistema, servisi sistema mogu postati nedostupni ovlašćenim korisnicima.

g) **Negacija transakcije** – Poslije izvršene transakcije, jedna od strana može da negira da se transakcija dogodila. Iako ovakav događaj može da nastupi usled greške, on uvijek proizvodi konflikte koji se ne mogu lako riješiti.

Najčešći vidovi transakcija u okviru elektronskog poslovanja su:

1. **između poslovnih subjekata**
2. **Poslovni subjekt - korisnik (kupac)**

   a) transakcije prema bankama (direktno raspolaganje korisnikovim računom)

   b) kupovina proizvoda preko web prodavnica, odnosno kupovina proizvoda putem Interneta (kreditne kartice i sl.)

Da bi se ostvarila neporecivost elektronskih transakcija, zaštita mora da osigura sledeće osnovne pretpostavke:

a) **Autentifikacija**

- Omogućava utvrđivanje identiteta korisnika, pri čemu su na raspolaganju tehnologije od korisničkog ID-a i statičke lozinke, preko tokena i biometrijskih tehnologija, do rešenja koja se temelje na asimetričnoj kriptografiji i sertifikatima, softverskim ili hardverskim (pametne kartice)

b) Privatnost

- Sprečava neautorizovani pristup podacima, ili presretanje istih tokom komunikacijskog procesa i ostvaruje se enkripcijom podataka

c) Integritet podataka

- osigurava se izvornost podataka, odnosno sprečavanje promene podataka primjenom digitalnog potpisa

Ispunjenje ovih pretpostavki osigurava se prije svega **kriptografski**, a time se postiže i pravno valjani dokaz o inicijatoru, kao i o samoj transakciji.

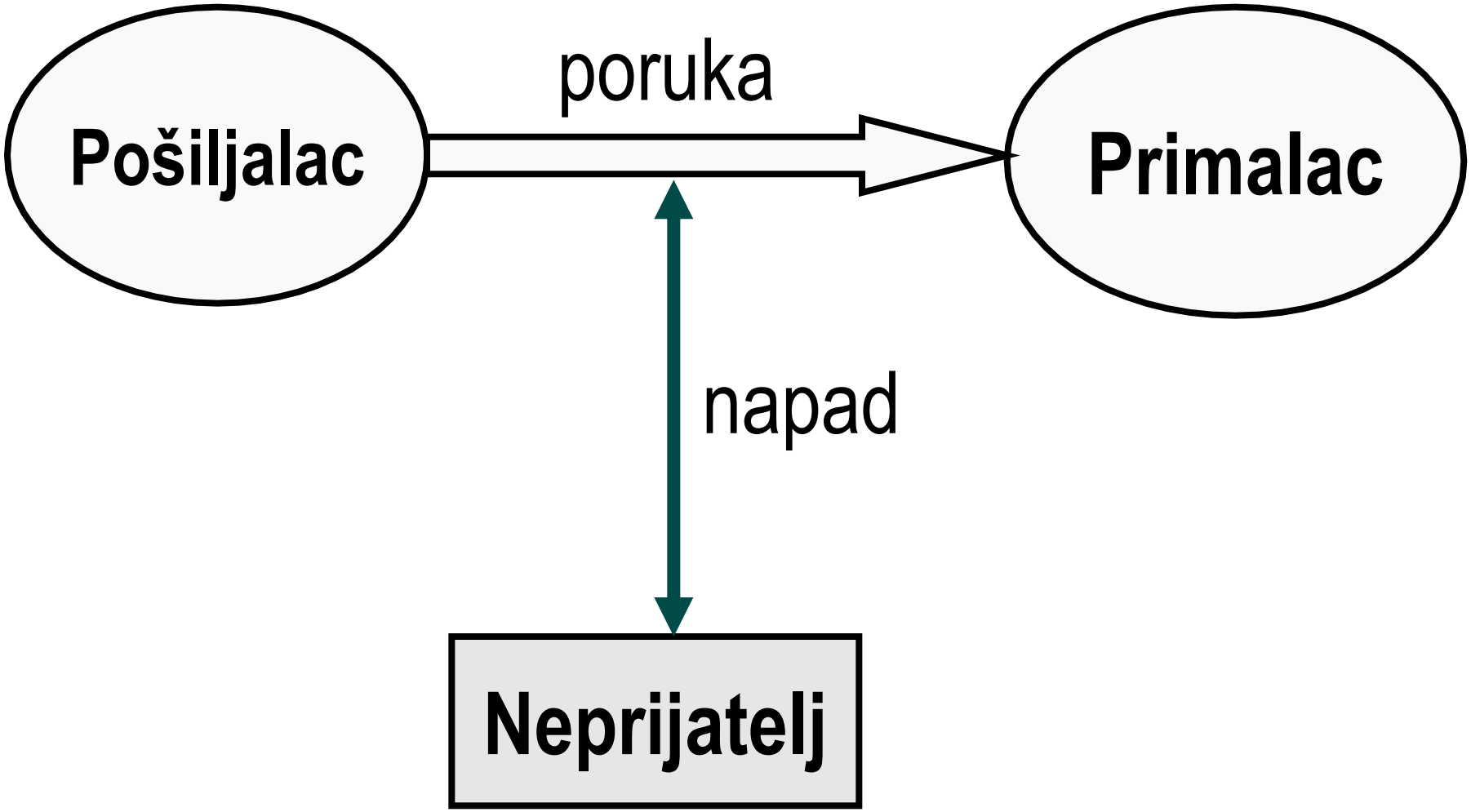
- Tehnologije koje su se nametnule kao opšte prihvaćeno rešenje za sigurnost elektronskih transakcija, odnosno realizaciju neporecivosti informacija su koncept **Digitalnog potpisa** i **Public Key Infrastrukture (PKI)**

OSNOVE KRIPTOGRAFIJE I KRIPTOGRAFSKE TEHNOLOGIJE

Kriptografija je stručni naziv za proces pretvaranja informacija u gomilu nepovezanih podataka koje niko osim primaoca ne može pročitati.

Namjena kriptografije je da:

- zaštiti memorisanu informaciju bez obzira ako je neko pristupio podacima
- zaštiti prenijetu informaciju bez obzira ako je prenos bio posmatran (“monitoring”)


Pošiljalac
poruka
Primalac
napad
Neprijatelj

Ciljevi kriptografije su da se obezbijedi:

- **Povjerljivost (tajnost**) – prevencija od neautorizovanog pristupa informacijama (obezbjeđuje privatnost za poruke)
- **Integritet** – prevencija od neautorizovanog menjanja informacija (obezbjeđuje potvrdu da poruka ostaje nepromijenjena)
- **Raspoloživost** – prevencija od neautorizovanog onemogućavanja pristupa informacijama ili resursima
- **Autentifikacija** – prevencija od lažnog predstavljanja (identifikacija izvora poruke i verifikacija identiteta osobe
- **Neporicanje** – prevencija od lažnog poricanja slanja date poruke/dokumenta (može se dokazati da poruka/dokument dolazi od datog entiteta iako taj entitet to poriče)

Mjere zaštite podrazumijevaju:

- **Prevencija** – preduzimanje preventivnih aktivnosti za zaštitu podataka i računarskih sistema od mogućeg uništenja
- **Detekcija** – otkrivanje kako je narušena zaštita, kada je narušena i ko je narušio
- **Reakcija** – preduzimanje aktivnosti koje dovode do restauracije podataka ili do restauracije računarskog sistema

Na konkretnom primeru e-Commerca pomenute mjere zaštite mogu podrazumijevati sledeće:

- **Prevencija** - Šifriranje broja kreditne kartice
- **Detekcija** - Listing svih transakcija u toku mjeseca urađenih datom kreditnom karticom
- **Reakcija** - Blokiranje stare kartice i podnošenje zahtjeva za izdavanje