Zasebnost na delovnem mestu – ZDA ali Evropa

Matej Kovačič
Fakulteta za družbene vede, IFIT

Nadzor na delovnem mestu

- Nadzor komunikacij zaposlenega:
  - "Ameriški pristop": zaposleni na delovnem mestu uporablja opremo, ki je last delodajalca, v delovnem času je plačan s strani delodajalca, zato službenih komunikacijskih sredstev in službenega časa ne sme zlorabljati v zasebne namene.
  - "Evropski pristop": zaposleni na delovnem mestu ni samo delavec, pač pa tudi človeško bitje in ima kot tak človekove pravice.

- Pravice "tretjih oseb"?
- Prometni podatki?

Ameriški pristop

primer Shoars proti Epson America Inc.

(Shoars v. Epson America Inc., No. (SWC) II2749 (Cal App. Dep't. Super. Ct. Dec 8, 1992))

- Administratorka e-poštnega sistema podjetja Epson je ugotovila, da eden izmed direktorjev prebira elektronsko pošto zaposlenih. Ko ga je s tem odkritjem soočila, je bila odpuščena.
- Alana Shoars je vložila tožbo, vendar pa se je podjetje branilo, da je sistem za elektronsko pošto v njihovi lasti in imajo zato pravico do njegovega upravljanja in nadzora, ali se uporablja samo v delovne namene ali ne.

Ameriški pristop

primer Shoars proti Epson America Inc.

(Shoars v. Epson America Inc., No. (SWC) II2749 (Cal App. Dep't. Super. Ct. Dec 8, 1992))

- Kalifornijsko sodišče njenim argumentom, da je njena zasebnost zaščitena s kalifornijsko ustavo, **ni pritrdilo** in sicer z obrazložitvijo, da ustava ščiti samo informacije, ki so osebne, ne pa tudi poslovnih komunikacij, poleg tega pa je **uporabljala opremo, ki je bila v lasti podjetja**.

Ameriški pristop

primer Bonita P. Bourke, et. al. proti Nissan Motor Corporation

(Bonita P. Bourke, et. al. v. Nissan Motor Corporation, No. 68-705 (Cal.Ct.App.1993))

- Leta 1993 je kalifornijsko prizivno sodišče razsodilo, da vpogled v elektronsko sporočilo, ki ga je uslužbenka poslala po omrežju podjetja, **ne pomeni** neupravičenega vdora v njeno zasebnost, ker je uslužbenka predhodno podpisala izjavo, v kateri se je zavezala, da bo elektronsko pošto uporabljala **izključno v službene namene**.

Ameriški pristop

primer McLaren proti Microsoft

(McLaren v. Microsoft, No. 05-97-00824 (Tex. Ct. App. 28. maj, 1999))

- Podjetje je pregledalo šifrirano elektronsko pošto zaposlenega (ki so jo pred tem dešifrirali), ki je bila shranjena v računalniku v mapi “Osebni imenik”.
- Zaposleni je sprožil sodni spor.
- Sodišče je v razsodbi dalo prav delodajalcu, in sicer z obrazložitvijo, da je interes delodajalca, da prepreči pošiljanje neprimerne elektronske pošte, **nad interesom zaposlenega do zasebnosti**.

Ameriški pristop

primer Smyth v. Pillsbury

(Smyth v. Pillsbury Co., 914 F.Supp. 97 (1996))

- Michael Smyth je leta 1994 enemu izmed sodelavcev poslal elektronsko sporočilo, v katerem je zapisal, da so njegovi predpostavljeni "*zahrbtne barabe*".
- Ker pa so njegovi predpostavljeni spremljali komunikacije svojih zaposlenih, so ga odpustili z obrazložitvijo, da so bili njegovi komentarji neustrezni in neprofesionalni.

Ameriški pristop

primer Smyth v. Pillsbury

(Smyth v. Pillsbury Co., 914 F.Supp. 97 (1996))

- Smyth se je pritožil na sodišče in trdil, da so mu v podjetju zagotovili zasebnost njegovih komunikacij, podjetje pa je trdilo nasprotno.
- Zvezno sodišče je primer zavrglo (in s tem dalo prav delodajalcu) in sicer z obrazložitvijo, da **tudi** če bi podjetje zaposlenemu res obljubilo tajnost komunikacij, sporno dejanje **ne posega v oškodovančevo zasebnost** na nepošten način.

Ameriški pristop

Electronic Communications Privacy Act, 1986

- ECPA v prvem poglavju, znanem tudi pod imenom ***Wiretap Act***, prepoveduje prestrezanje elektronskih telekomunikacij, pri čemer je 'prestrezanje' definirano kot:

"*zaznavanje izžarevanja [signala] ali druga pridobitev vsebine žice oziroma elektronske ali ustne komunikacije, ki poteka s pomočjo uporabe kakršnekoli elektronske, mehanične ali druge naprave*".

Ameriški pristop

Electronic Communications Privacy Act, 1986

- Prestrezanje po ECPA torej poteka **hkrati s prenosom**.
- Vendar pa za nadzorovanje elektronske pošte ni treba uporabljati sočasnega prestrezanja.

- Če delodajalec dostopa do strežnika, v katerem je shranjeno elektronsko sporočilo, s tem zaobide prepoved sočasnega prestrezanja.

Ameriški pristop

Electronic Communications Privacy Act, 1986

- ECPA v drugem poglavju, znanem pod imenom ***Stored Communications Act***, ki prepoveduje dostop do shranjenih elektronskih sporočil brez soglasja nadzorovane osebe, iz prepovedi eksplicitno izključuje:

  "osebe, ki zagotavljajo (ang. to provide) žično ali elektronsko komunikacijsko storitev"

- Iz prepovedi so torej izvzeti delodajalci, ki imajo v lasti komunikacijsko opremo podjetja.

Ameriški pristop

Electronic Communications Privacy Act, 1986

- ECPA delodajalcem v vsakem primeru dovoljuje nadzor komunikacij, ki zadevajo poslovanje podjetja (ne pa tudi zasebnih pogovorov).
- Delodajalec po ECPA lahko posluša pogovor vsaj nekaj časa, da lahko ugotovi, **ali gre za poslovni ali zasebni pogovor**.
- Za razliko od telefonskega pogovora pa je dostop do elektronske pošte popoln (ne delen ali časovno omejen), zato je nadzor elektronske pošte laže upravičiti.

Evropski pristop

Odločitve Evropskega sodišča za človekove pravice

(Halford proti Veliki Britaniji, Copland proti Veliki Britaniji)

- **Halford proti Veliki Britaniji** iz leta 1997: ESČP je v razsodbi izrecno zapisalo, da zaposleni na delovnem mestu upravičeno pričakuje zasebnost.
- **Copland proti Veliki Britaniji** iz leta 2007: ESČP je v zvezi z uporabo interneta in elektronske pošte na delovnem mestu delavki priznalo širok krog pravice do zasebnosti in presodilo, da je delodajalec neupravičeno posegal v njeno zasebnost. Ključni element sodbe je, da delavka ni bila vnaprej opozorjena, kdaj in v kakšnih primerih lahko delodajalec nadzira e-pošto.

Evropski pristop

Odločitve Evropskega sodišča za človekove pravice

(Niemitz proti Nemčiji)

- **Niemietz proti Nemčiji** iz leta 1992: "*Sodišče ne smatra, da je mogoče ali nujno poizkusiti podati izčrpno definicijo 'zasebnega življenja'"*
- "*Spoštovanje zasebnega življenja mora vsebovati tudi določeno stopnjo pravice do* ***vzpostavljanja in razvijanja odnosov z drugimi človeškimi bitji****."*
- "*Poleg tega se zdi, da ni načelnega razloga, zakaj bi ta pojem 'zasebnega življenja'* ***izključeval profesionalne ali poslovne*** *dejavnosti [posameznika]..."*

Evropski pristop

Odločitve Evropskega sodišča za človekove pravice

(Lambert proti Franciji, Kopp proti Švici)

- Evropsko sodišče za človekove pravice je v primeru **Lambert proti Franciji** iz leta 1998 poudarilo, da glede tajnosti komunikacij ni razlike med lastnim telefonskim priključkom ali telefonskim priključkom tretje osebe.
- V primeru **Kopp proti Švici** iz leta 1998 pa je ESČP zapisalo, da so zaščiteni tudi klici iz poslovnih prostorov ter v poslovne prostore.

Evropski pristop

Odločitev Kasacijskega sodišča Francije

(Societe Nikon France, SA v. Onof, št. 99–42.942 iz leta 2001)

- *"Delodajalec, ki bere sporočila, ki jih zaposleni pošilja ali sprejema preko službenega računalnika, krši temeljne pravice delavca, kot jih določa 8. člen Evropske konvencije o človekovih pravicah..."*
- *"To velja **ne glede na to**, ali je bil delavec vnaprej seznanjen, da službenega računalnika ne sme uporabljati v neslužbene namene..."*

Evropski pristop

Odločitev Kasacijskega sodišča Francije

(Societe Nikon France, SA v. Onof, št. 99–42.942 iz leta 2001)

- "*Podjetje ali druge ustanove ne smejo biti mesta, kjer bi delodajalci arbitrarno in brez omejitev izvajali svoje diskrecijske pravice;* ***ne smejo postati okolja totalnega nadzora****, kjer temeljne človekove pravice nimajo veljave...*"
- "*Menimo, da je splošna popolna prepoved uporabe e-pošte v neslužbene namene* ***nerealna in krši pravno načelo sorazmernosti***."

Ustava Republike Slovenije

37. člen - varstvo tajnosti pisem in drugih občil

- "Zagotovljena je tajnost pisem in drugih občil.
- Samo **zakon** lahko predpiše, da se **na podlagi odločbe sodišča** za **določen čas** ne upošteva varstvo tajnosti pisem in drugih občil in nedotakljivost človekove zasebnosti, če je to nujno za uvedbo, ali potek kazenskega postopka ali za varnost države."

Ustavno sodišče RS

Odločba Ustavnega sodišča RS Up-472/02

(Uradni list RS, št. 114/2004)

- Ustavno sodišče RS je odločalo o snemanju razgovora s strani zasebnika in uporabi tega posnetka v kasnejšem civilnem sodnem postopku.
- "*Posnetka oziroma tonskega zapisa telefonskega pogovora tudi ni mogoče enačiti z zapiski o pogovoru. Gre namreč za* ***bistveno kakovostno razliko****... Kot je že bilo poudarjeno, daje tonski zapis oblast nad tujo osebo oziroma njeno osebno dobrino, ker omogoča ponovitev (ponovno predvajanje). Če je torej to storjeno brez vednosti prizadete osebe, je s tem* ***poseženo v izključno pravico osebe, da sama razpolaga*** *s svojo besedo oziroma z glasom.*"

Ustavno sodišče RS

Odločba Ustavnega sodišča RS Up-106/05

(Uradni list RS, št. 100/2008)

- Policija je pritožniku med zakonito izvedeno preiskavo zasegla mobilni telefon ter ga nato, vključno s SIM kartico pregledala. V kazenskem postopku pritožnik je zatrjeval, da so bili podatki, ki so se nahajali na zaseženi kartici SIM, pridobljeni brez odredbe preiskovalnega sodnika
- Ustavno sodišče je odločilo, da **poseg v svobodo komuniciranja ni dovoljen brez predhodnega dovoljenja sodišča** ter s tem dalo prav pritožniku.

Kazenski zakonik RS

139. člen KZ-1 - kršitev tajnosti občil

(2) Z denarno kaznijo ali z zaporom do enega leta se kaznuje:

2) kdor se z uporabo **tehničnih sredstev** neupravičeno seznani s sporočilom, ki se prenaša po telefonu ali s kakšnim drugim **telekomunikacijskim sredstvom**;

...

(3) Enako se kaznuje, kdor s katerim od dejanj, ki so navedena v prvem in drugem odstavku tega člena, **omogoči drugemu**, da se neposredno seznani z vsebino sporočila ali pošiljke.

...

(5) Če stori dejanje iz prejšnjih odstavkov tega člena uradna oseba z zlorabo uradnega položaja ali uradnih pravic, poštni **ali drug delavec**, ki mu je zaupano prevzemanje, prenos ali predaja tujih pisem, tujih brzojavk ali kakšnih drugih pisanj ali pošiljk, se kaznuje z zaporom od treh mesecev do petih let.

Prometni podatki

- Evropsko sodišče za človekove pravice je v primeru **Malone proti Veliki Britaniji** leta 1984 presodilo, da so prometni podatki integralni element telefonskih komunikacij.
- Vrhovnosodišče ZDA je leta 1979 v primeru **Smith proti Maryland** presodilo, da prometni podatki o telefonskih pogovorih niso zaščiteni s *Četrtim amandmajem*, s čimer so uvedli ločevanje prometnih podatkov od same vsebine komunikacije.
- Evropska Unija: **Direktiva o obvezni hrambi prometnih podatkov** v EU zahteva obvezno hrambo prometnih podatkov vendar je dostop do prometnih podatkov strogo omejen.

Prometni podatki

- Po **Zakonu o varstvu osebnih podatkov** so prometni podatki osebni podatki:
  - 6. člen: Osebni podatek je katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen. Posameznik je določena ali določljiva fizična oseba, na katero se nanaša osebni podatek.
- Vpogled v prometne podatke pomeni obdelavo osebnih podatkov:
  - 6. člen: Obdelava osebnih podatkov pomeni kakršnokoli delovanje ali niz delovanj, ki se izvaja v zvezi z osebnimi podatki.

Prometni podatki

Mnenje Informacijskega pooblaščenca glede nadzora e-pošte

(http://www.ip-rs.si/pogosta-vprasanja/varstvo-osebnih-podatkov/)

- Sama vsebina e-pošte je varovana neposredno na podlagi 37. člena Ustave RS, vendar za ta del elektronske pošte Pooblaščenec ni pristojen (možnost vložitve odškodninske tožbe ali uvedba kazenskega postopka).
- Teorija je iz nekaterih primerov Evropskega sodišča za človekove pravice (npr. Halford v. Velika Britanija) izvedla tudi predpostavko, da so **varovani tudi prometni podatki**, torej komu ste poslali elektronsko pošto in kdo jo je poslal vam. To pa je tudi **zbirka osebnih podatkov** in za morebiten vpogled vanjo mora delodajalec pridobiti **privolitev zaposlenega**.

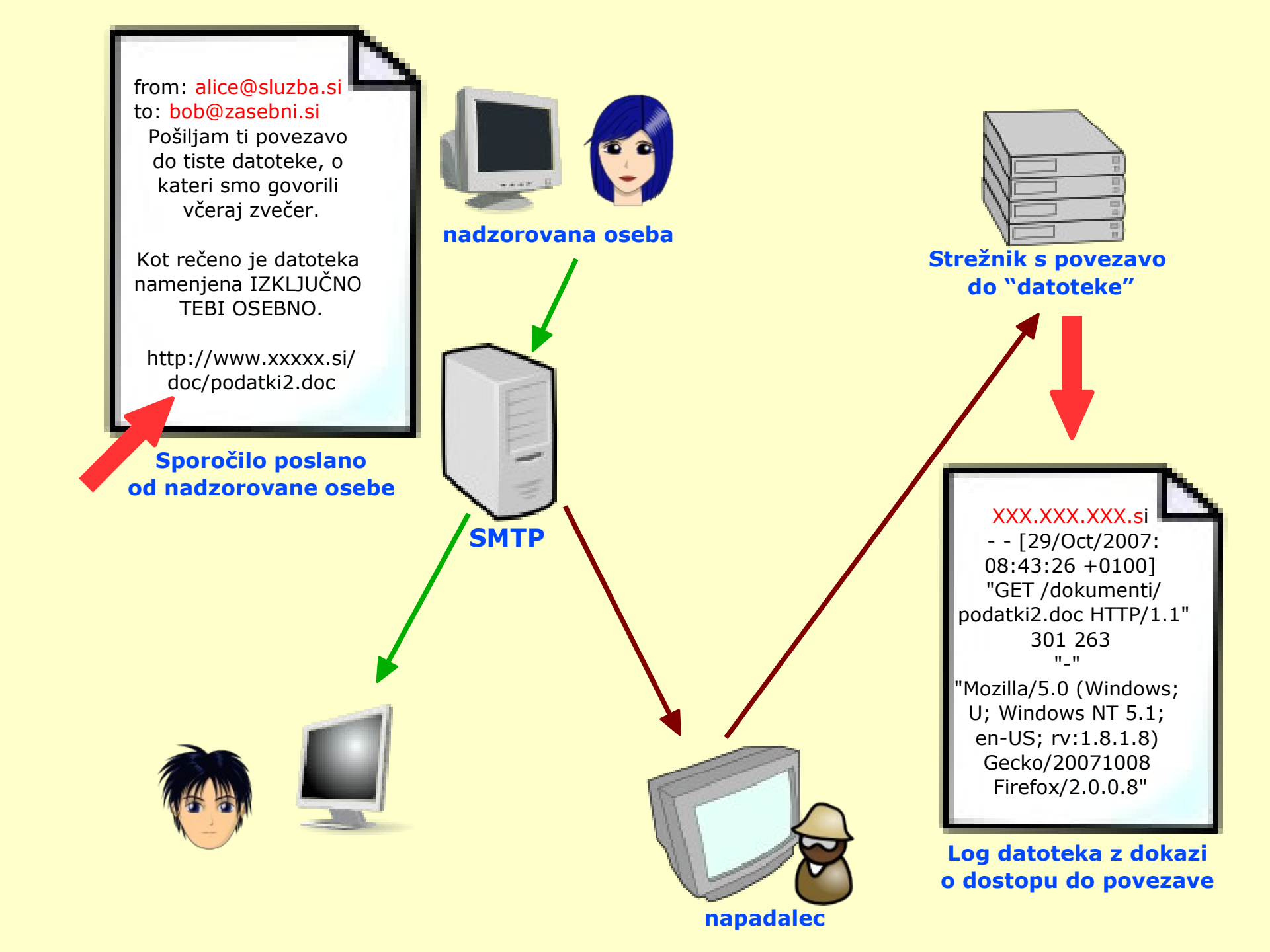
Prometni podatki

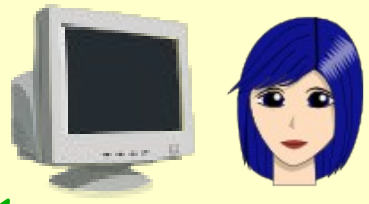
Mnenje Informacijskega pooblaščenca glede nadzora telefona

(http://www.ip-rs.si/pogosta-vprasanja/varstvo-osebnih-podatkov/)

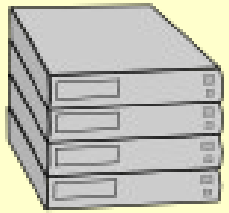
- Pridobitev izpiska klicev izhaja iz lastninske pravice delodajalca. A v trenutku, ko bi delodajalec začel ugotavljati, komu klicane številke pripadajo, to pomeni **obdelavo osebnih podatkov**.
- To je torej meja, do katere lahko delodajalec obdeluje izpisek klicev. Prekoračitev zneska, do katerega lahko posameznik uporablja službeni telefon, je potrebno ugotavljati tako, da se ne razkriva osebnih podatkov.
- Za delodajalce je priporočljivo, da pravila telefoniranja določijo vnaprej in na podlagi pisne privolitve posameznika.

Primer razkritja nezakonitega prestrezanja e-pošte s strani slovenskega delodajalca v letu 2007


from: alice@sluzba.si
to: bob@zasebni.si
Pošiljam ti povezavo do tiste datoteke, o kateri smo govorili včeraj zvečer.
Kot rečeno je datoteka namenjena IZKLJUČNO TEBI OSEBNO.
http://www.xxxxx.si/doc/podatki2.doc
Sporočilo poslano od nadzorovane osebe
nadzorovana oseba
SMTP
Strežnik s povezavo do "datoteke"
XXX.XXX.XXX.si - - [29/Oct/2007:08:43:26 +0100] "GET /dokumenti/podatki2.doc HTTP/1.1" 301 263 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.8) Gecko/20071008 Firefox/2.0.0.8"
Log datoteka z dokazi o dostopu do povezave
napadalec



nadzorovana oseba

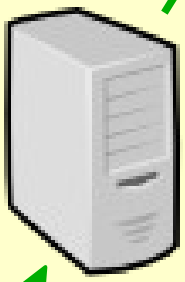


Strežnik s povezavo do "datoteke"

from: bob@zasebni.si
to: alice@sluzba.si

Prosim poglej tole v zvezi s sinočnjo debato in mi sporoči, če se strinjaš. Greš na spletno stran http://www.xxxxx.org in se prijaviš z uporabniškim imenom katarina in geslom geslo123.

Sporočilo poslano nadzorovani osebi

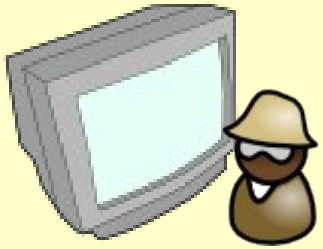


POP3

uporabniško ime: **katarina**
geslo: **geslo123**

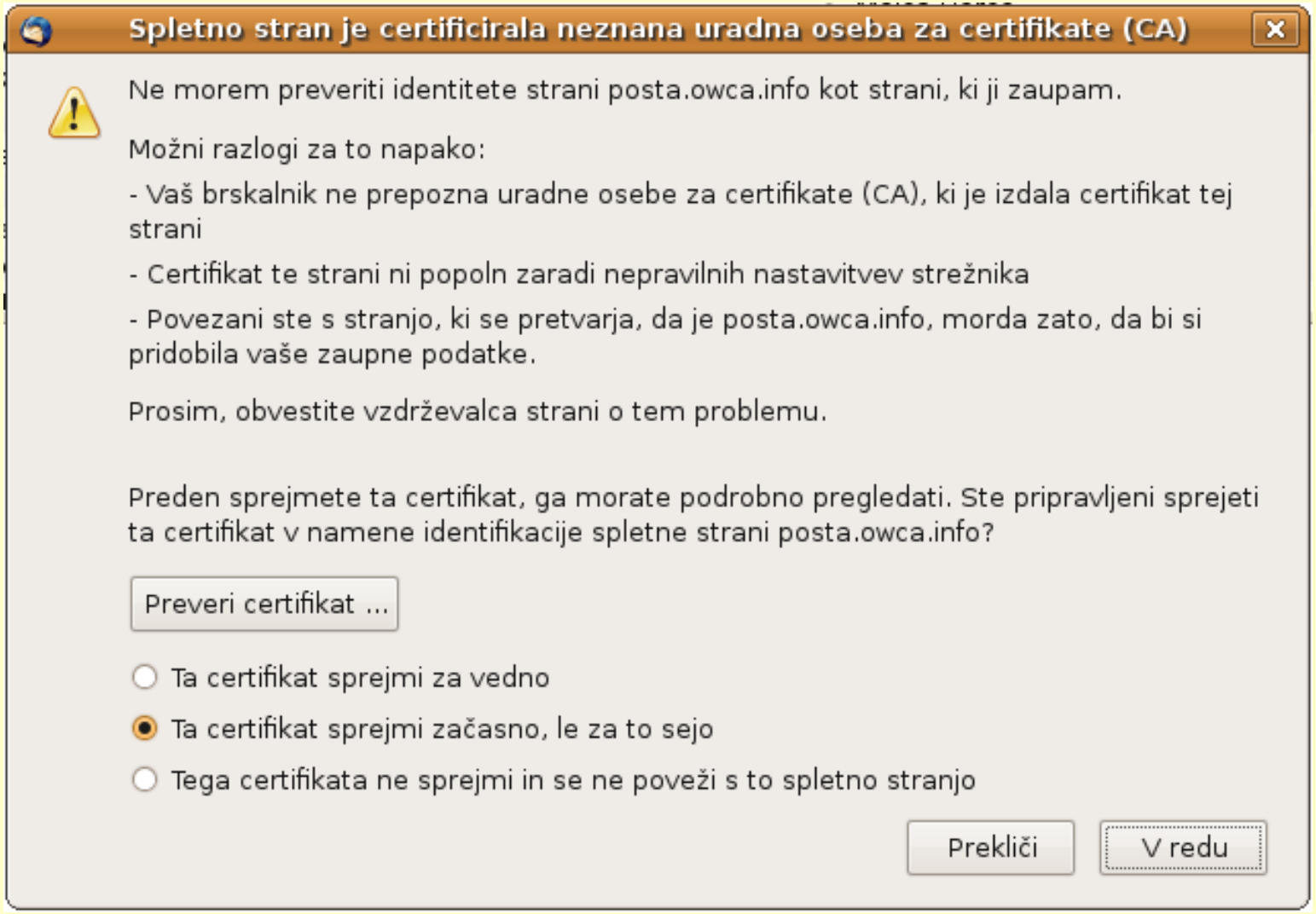
xxx.xxx.xxx.si - katarina [29/Oct/2007: 08:14:47 +0100] "GET / HTTP/1.1" 200 1117 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.8) Gecko/20071008 Firefox/2.0.0.8"

Dnevniška datoteka z dokazi o dostopu do povezave

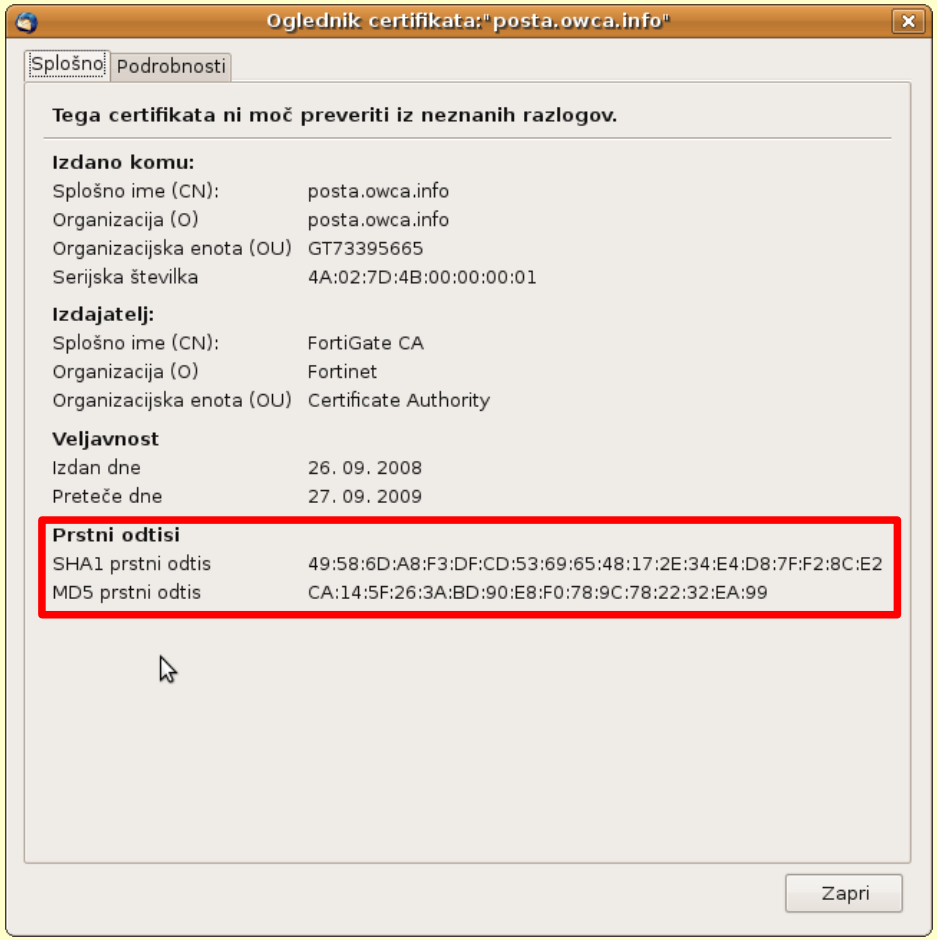


napadalec

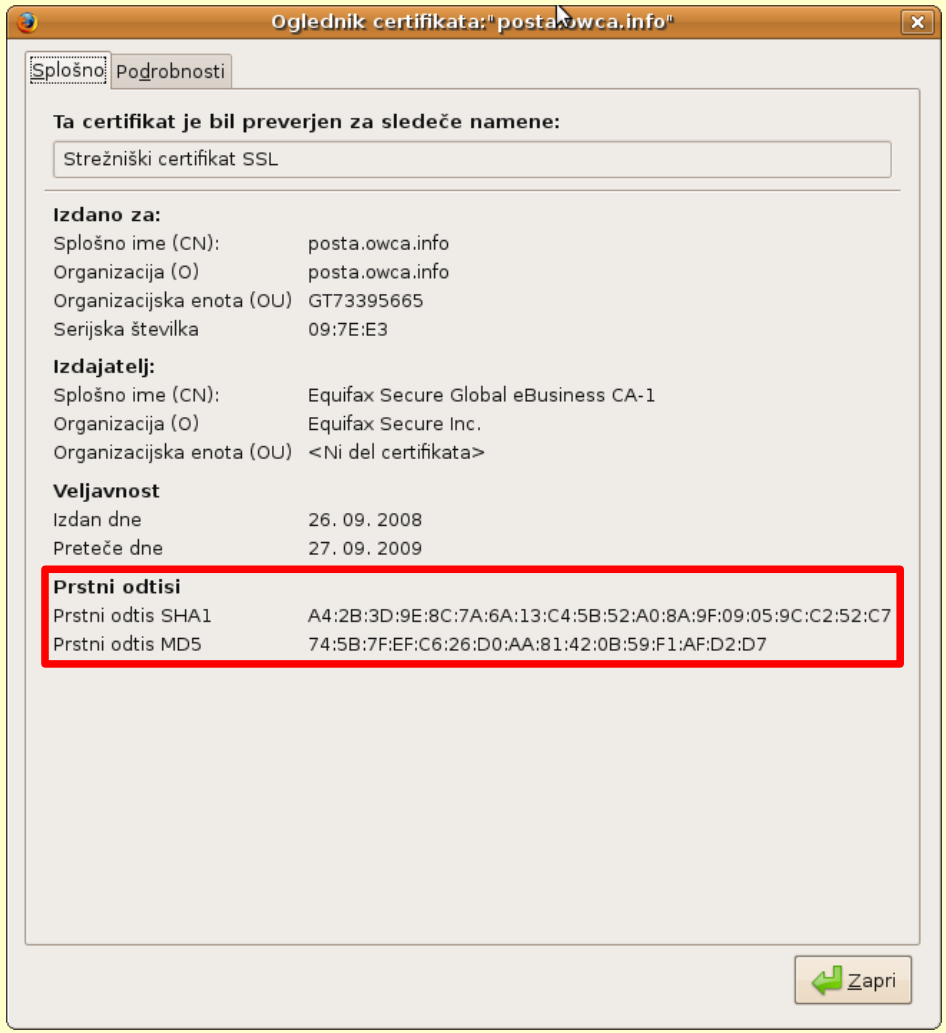
Primer razkritja nadzora internetnih komunikacij s strani slovenskega delodajalca v letu 2009


Spletno stran je certificirala neznana uradna oseba za certifikate (CA)
Ne morem preveriti identitete strani posta.owca.info kot strani, ki ji zaupam.
Možni razlogi za to napako:
- Vaš brskalnik ne prepozna uradne osebe za certifikate (CA), ki je izdala certifikat tej strani
- Certifikat te strani ni popoln zaradi nepravilnih nastavitvev strežnika
- Povezani ste s stranjo, ki se pretvarja, da je posta.owca.info, morda zato, da bi si pridobila vaše zaupne podatke.
Prosim, obvestite vzdrževalca strani o tem problemu.
Preden sprejmete ta certifikat, ga morate podrobno pregledati. Ste pripravljeni sprejeti ta certifikat v namene identifikacije spletne strani posta.owca.info?
Preveri certifikat ...
Ta certifikat sprejmi za vedno
Ta certifikat sprejmi začasno, le za to sejo
Tega certifikata ne sprejmi in se ne poveži s to spletno stranjo
Prekliči
V redu

7. maj 2009

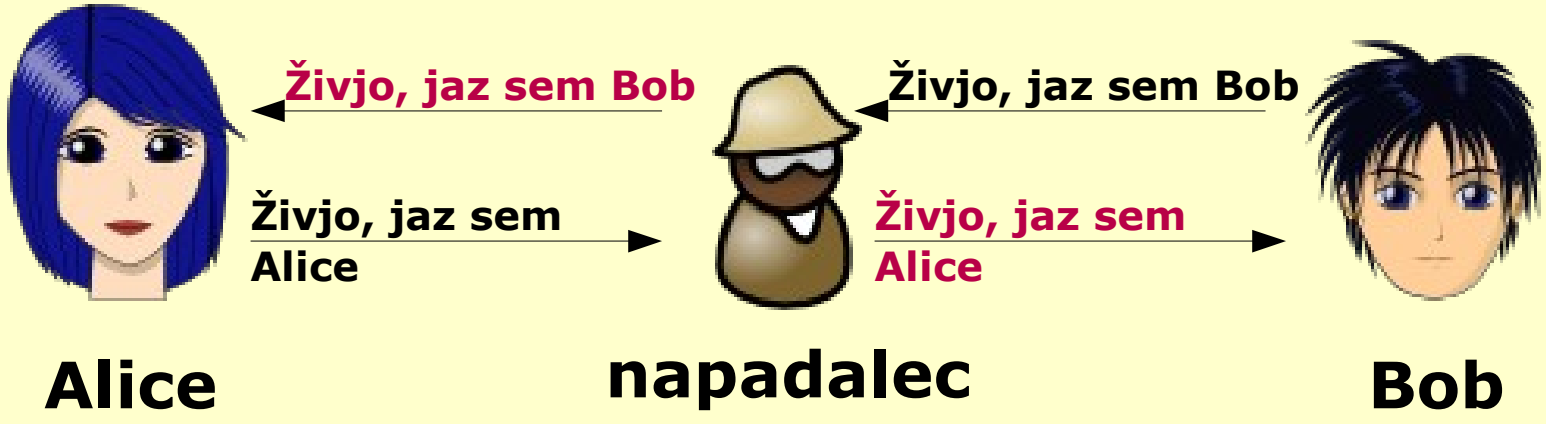


lažni certifikat

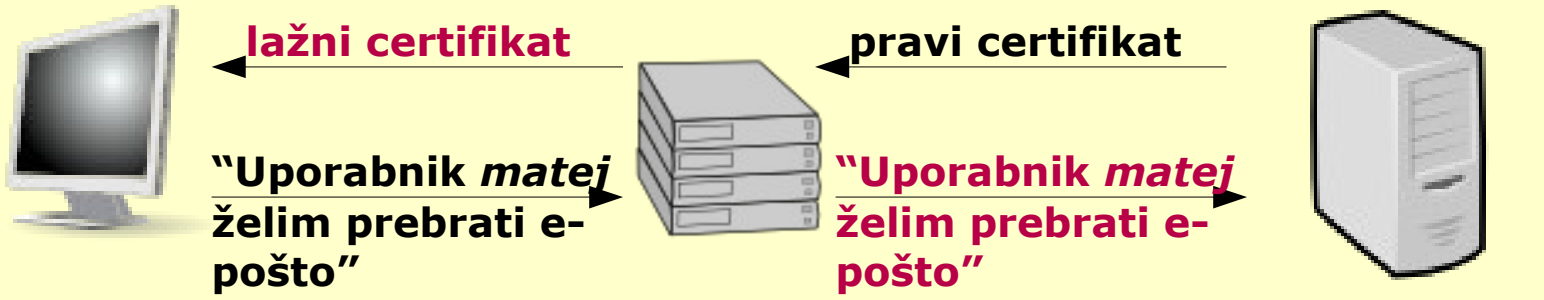


pravi certifikat

Napad s posrednikom (MITM - man-in-the-middle)



Napad s posrednikom (MITM - man-in-the-middle)



Kazenski zakonik RS

221. člen KZ-1 - napad na informacijski sistem

(1) Kdor vdre v informacijski sistem ali kdor **neupravičeno prestreže podatek ob nejavnem prenosu** v informacijski sistem ali iz njega, se kaznuje z zaporom do enega leta.

(2) Kdor podatke v informacijskem sistemu **neupravičeno uporabi**, **spremeni**, preslika, prenaša, uniči ali v informacijski sistem **neupravičeno vnese kakšen podatek**, ovira prenos podatkov ali delovanje informacijskega sistema, se kaznuje za zaporom do dveh let.

(3) Poskus dejanja iz prejšnjega odstavka je kazniv.

(4) Če je z dejanjem iz drugega odstavka tega člena povzročena velika škoda, se storilec kaznuje z zaporom od treh mesecev do petih let.

Vprašanja?