Fakulteta za elektrotehniko, računalništvo in informatiko

Revidiranje informacijskih sistemov

ITK 3 UN IS, ITK 3 UN TK

Predavanje 1 od 14

Maribor, 3. oktober 2014

Vsebina prvega predavanja

- Predstavitev
- Način dela
- Komunikacija
- Izpit
- Uvod v predmet
- Zaključek / povzetek

Predstavitev

- Predmeta
- Predavatelja
- Asistentke
- Slušateljev

Predstavitev predmeta - namen

- Spoznati namen in cilje revizije IS.
- Seznaniti se s postopki, pravili, standardi in zakonodajo.
- Ponoviti ključna strokovna področja, ki jih zajema revizija IS.
- Omogočiti sodelovanje v različnih vlogah pri izvajanju revizij

Predstavitev predavatelja

doc.dr. Boštjan Delak, CISA, CIS, aktiven preizkušeni revizor IS,
samostojni svetovalec
docent za področje informatike

ITAD, Revizija in svetovanje d.o.o.
e-pošta: bostjan.delak@itad.si
Tel: 0599-44500

www.itad.si

sekcija za upravljanje varovanja informacij

www.suvi.si

Predstavitev predavatelja

Delovne izkušnje:

- 2008 – do danes ITAD, revizija in svetovanje d.o.o.
- 1996 – 2008 Nova ljubljanska banka d.d., Ljubljana
- 1992 – 1996 IBM Slovenija
- 1986 – 1992 Intertrade – zastopstvo IBM
- 1982 – 1986 ISKRA Avtomatika - Sistemi

Predstavitev predavatelja

Članstva:

- ISACA - Information System Audit and Control Association od 2004
- AIS – Association for Information Systems od 2008
- Slovensko društvo Informatika od 2008

Interes:

- revidiranje IS
- analize IS
- skrbni pregledi IS
- upravljanja znanja IS

Prosti čas:

- Nordijska hoja, SUDOKU, urejanje vrta

Predstavitev asistentke

asist. Katja Kous, univ.dipl. inž. rač. in inf.

UM, FERI, Inštitut za informatiko
e-pošta: katja.kous@um.si
Kabinet: G2.1N-14
Tel: 02-220 7402
Govorilne ure: ponedeljek, 12.00 – 14.00

http://www.feri.uni-mb.si

Predstavitev asistentke

Delovne izkušnje:

• 2008 – do danes	UM, FERI, Inštitut za informatiko
• 2006 – 2007	študentsko delo v podjetju B2 d.o.o.
• 2005 – 2008	študentsko delo na UM FERI, Inštitutu za informatiko

Predstavitev asistentke

Članstva:

- Članica SIST/TC ITC (2008 – danes)
- Članica itSMf Slovenija (2008 – danes)

Interes:

- uporabniška izkušnja IT rešitev
- modeliranje poslovnih procesov
- metodologije vodenja IT projektov
- strateško vodenje informatike

Predstavitev slušateljev

Ime in priimek

Izkušnje na področju IS

Izkušnje z revizijami in revidiranjem IS

Interes:

Prosti čas: *ni obvezno*

Način dela

- Predavanja
- Predstavitve
- Vaje
- Literatura

Način dela - predavanja

- Vsak petek
  - Med 3.10.2014 in 19.12.2014 - med 13.00 in 16.00
  - 3 šolske ure – z dvema krajšima odmoroma (7-8 minut)
  - Med 9.1.2015 in 23.1.2015 – *med 12.00 in 16.00 ?? (križanje z vajami (11.30 – 13.) – potrebno razrešiti v referatu)*
  - 4 šolske ure – s tremi krajšimi odmori (7-8 minut)?

Način dela - predavanja

- Prisotnost
  - Uradno neobvezna
  - Neuradno

  - Za mojo statistiko in moj arhiv – lista prisotnosti

Način dela - predstavitve

- Predstavitve (pdf format) predavanj bo naložen na Moodle UM najkasneje v sredo zvečer pred posameznimi predavanji
- Ta predstavitev bo na Moodle UM v naslednjih dneh
- Na Moodle UM bodo naloženi tudi:
  - dokumenti, ki jih bomo obravnavali med predavanji,
  - fotografije zapisov na tabli,
  - drugo

Način dela - vaje

- Prisotnost
  - Obvezna (min 80%)
  - Preverjanje prisotnosti
  - Trening na primerih
  - Samostojno delo na projektu

Način dela - vaje

- Vsak ponedeljek
  - Med 01.10.2014 in 23.01.2015 - med 10.00 in 11.30 v učilnici Hertz

Način dela - literatura

- Uradna literatura
  - Mednarodni standardi za strokovnjake revidiranja, kontrol in dajanja zagotovil na področju IT
  - Hierarhija pravil revidiranja informacijskih sistemov (Uradni list RS. št. 40/2011)
  - CISA Review Manual (ISACA)
  - Auditor's Guide to IS Auditing (Cascarino)
  - Audit Planning: Risk Based Approach (Pickett)
  - IT Risk, (Westerman, Hunter)
  - ISO standardi
  - COBIT
  - Literatura za posamezna področja dela

Način dela - literatura

- Praktična literatura
  - zapiski predavanj
  - prosojnice predavanj
  - iskanje po spletnih virih

Komunikacija

- Sodelovanje
- Spremembe začetka predavanj
- Predstavitve
- Vprašanja
- Govorilne ure
- Obvestila

Komunikacija - sodelovanje

Komunikacija - predavanja

- Spremembe začetka predavanj
  - načrtovana ob 13:00 (2014) oziroma ob 12:00 (2015)
- v primeru višje sile na dan predavanj – asistentka
- v primeru višje sile – obvestila na Moodle UM predmeta (nasvet: četrtek popoldan poglejte na Moodle UM predmeta)

Komunikacija - predstavitve

- Predstavitve v pdf obliki:
  - bodo naložene na Moodle UM predmeta najkasneje v sredo zvečer pred naslednjimi predavanji
  - ta predstavitev bo naložena na Moodle UM predmeta v prihodnjih dneh

Komunikacija - vprašanja

- Posredovanje vprašanj:
  - za tekoče predavanje: takoj ali na koncu predavanja
  - ostala predavanja: po e-pošti
  - glede izpita: po e-pošti
  - glede literature: po e-pošti

Komunikacija – govorilne ure

- Govorilne ure:
  - Termin bo usklajen in sporočen na Moodle UM do sredine oktobra 2014
  - Predvidoma ob petkih

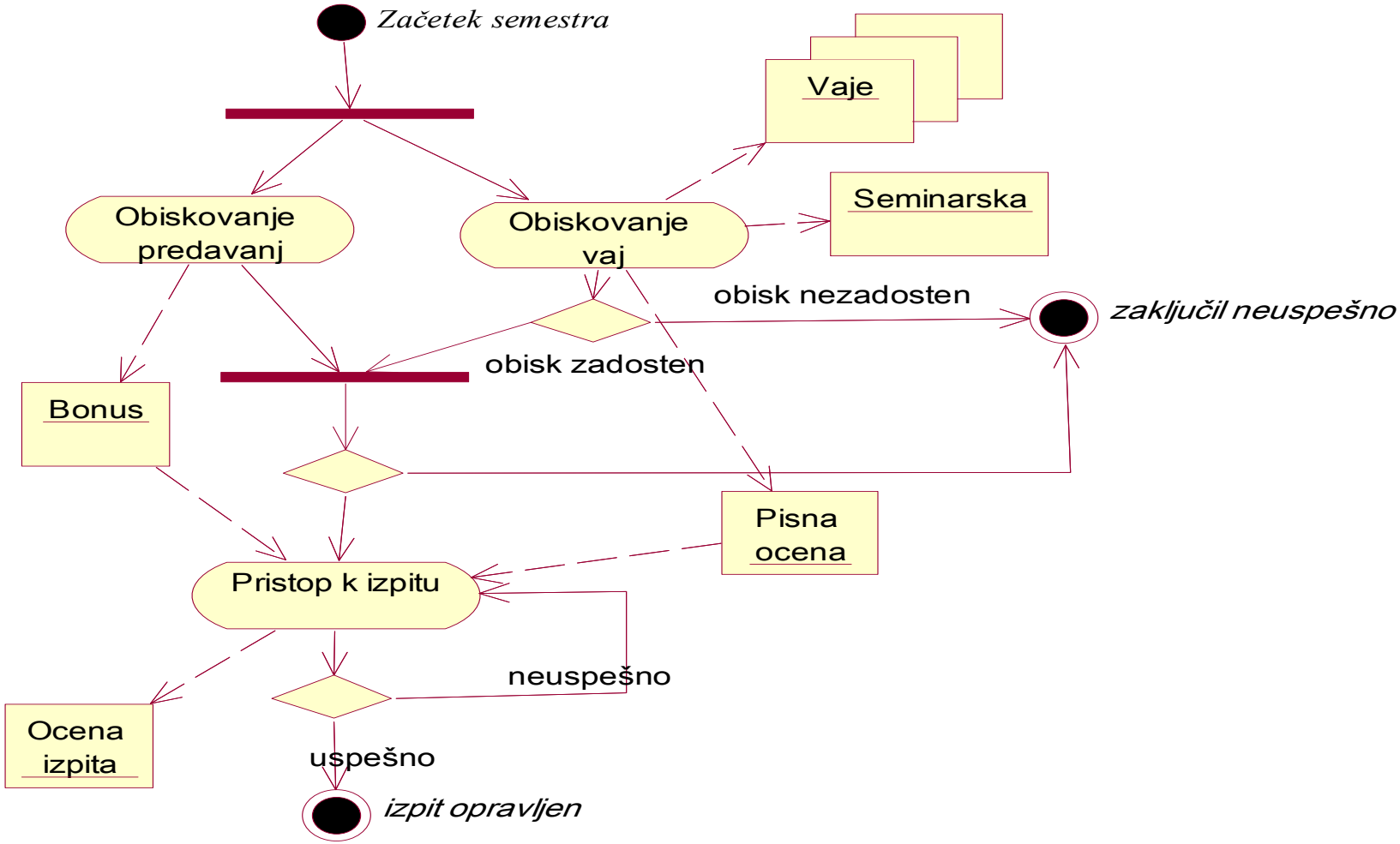
Komunikacija – obvestila

- Obveščanje:
  - po e-pošti
  - na telefonsko številko ITAD, revizije in svetovanje d.o.o. in pustite sporočilo

Izpit

- Potek dela
- Ocenjevanje

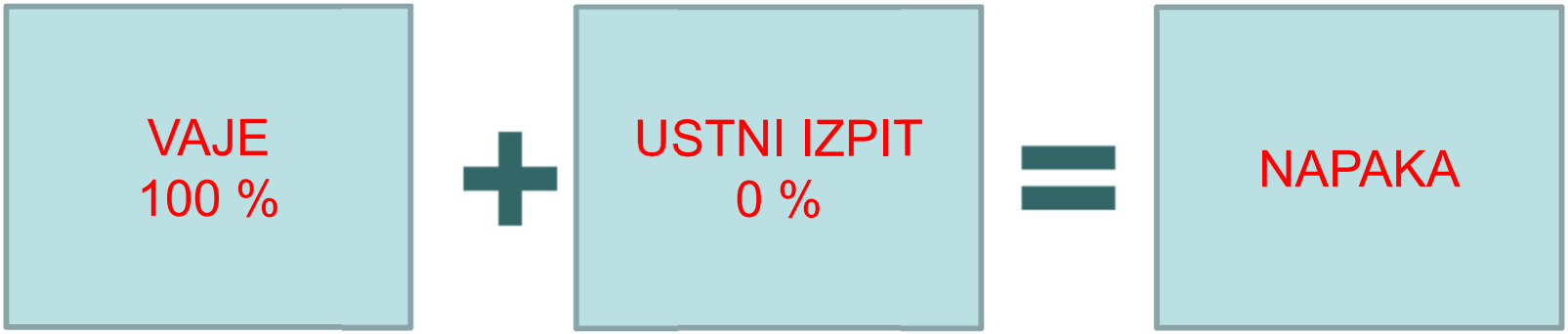
Izpit – potek dela



Izpit - ocenjevanje

- Ustni izpit 40 %
- Laboratorijske vaje 20 %
- Pisni izpit 40 %

} 60 %



Izpit - ocenjevanje

- Pisni izpit
- Kolokvij I – konec novembra / začetek decembra
- Kolokvij II - ko bodo izpitni roki

Uvod v revidiranje

- Motivacija
- Primeri
- Terminologija

Uvod v revidiranje - motivacija

Nepooblaščena uporaba

- Davčni zavezanec, zaposlen v Zavarovalnici Triglav, je nepooblaščeno želel spremeniti svoje podatke o vzdrževanih članih, pri čemer je ob pomoči posebne kode, ki je namenjena izplačevalcu, Zavarovalnici Triglav, zbrisal podatke o vzdrževanih članih za vse zaposlene v Triglavu. Tu ni šlo za vdor v Dursov informacijski sistem, ampak napako.

- Vir: Finance 4.4.2008

Uvod v revidiranje - motivacija

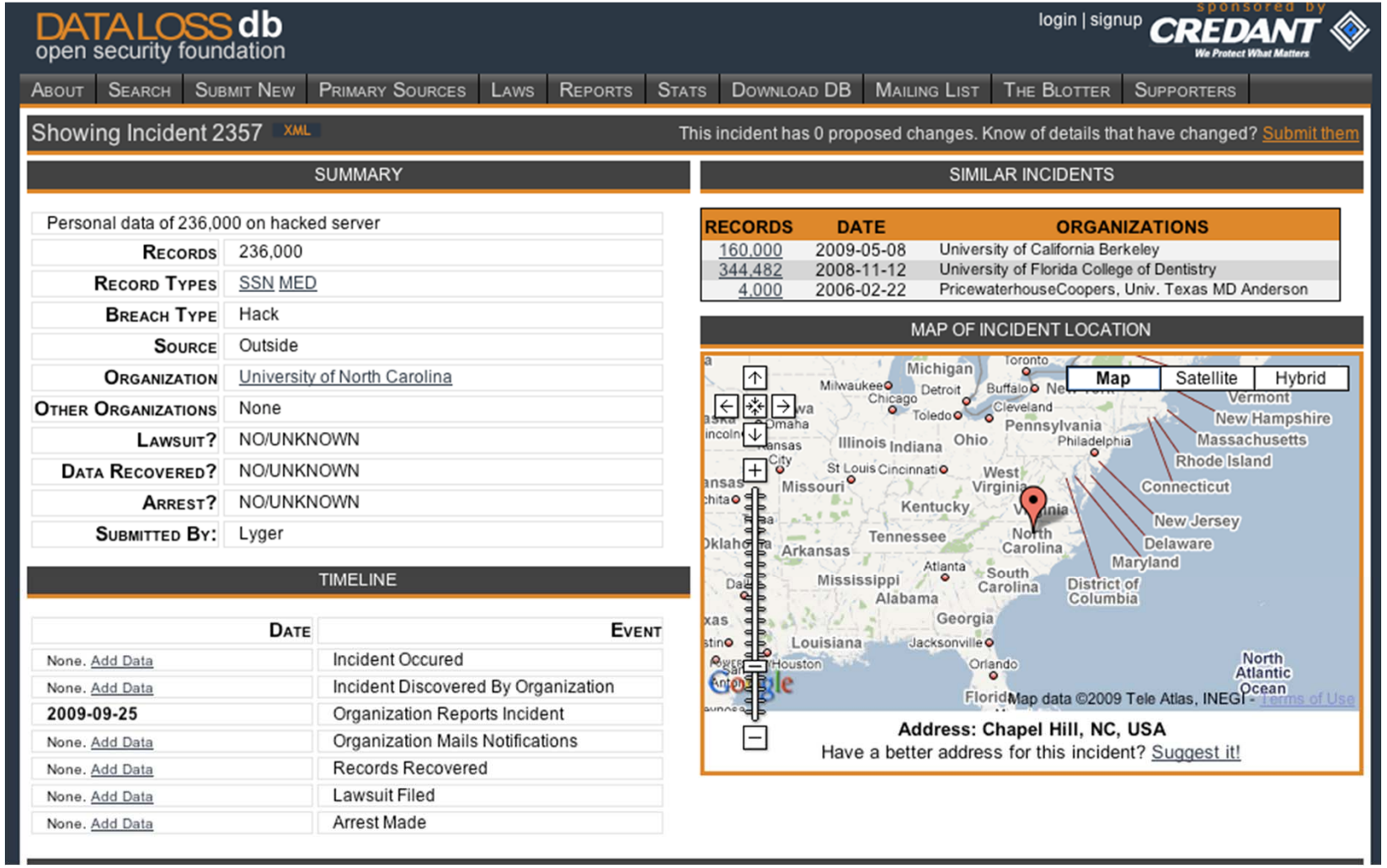
Prevare

- ✓ Kako slabo so varovani računalniški oziroma informacijski sistemi, se pogosto zavemo šele tedaj, ko nas to pošteno udari po žepu. To naj bi na lastni koži izkusili kupci Merkurjeve trgovine v Kranju, ki so blago plačevali s kreditnimi karticami. Spretni hekerji naj bi namreč med 13. in 19. februarjem vdrli v sistem POS-terminala, kjer so bile shranjene številke kreditnih kartic Merkurjevih kupcev. S pridobljenimi številkami naj bi nepridipravi na Nizozemskem dvigovali v povprečju 200 evrov oziroma dovoljeni znesek dnevnega limita.

Vir: Računalnike novice 1.3.2007

Uvod v revidiranje - motivacija

Izguba podatkov



Uvod v revidiranje - motivacija

Virusi

- ✓ The report pointed out the continuing rise of incidents reported by federal agencies and, in particular the ‘I Love You’ virus last May, that federal computer security “continued to be fraught” with weaknesses. The virus caused message system disruptions at public agencies and private companies.

Uvod v revidiranje - motivacija

Posredna škoda

Spletni Klik je spet varen! (Foto: POP TV)

Težave, ki so se pojavile pri vstopu do spletne banke Klik, so bile povezane z osamljenim primerom. Šlo je za neustrezno zaščito in ne za vdor v spletni bančni sistem, pojasnjujejo v Novi ljubljanski banki. Kot so povedali, jih je o pojavu ponarejene vstopne strani spletne poslovalnice NLB Klik obvestila stranka. Predpogoj, da se ponarejena stran pokaže na zaslonu, je okužen osebni računalnik, pojasnjuje **Mojca Strojan**, vodja odnosov z javnostmi pri NLB. Stranka ponarejeni strani ni nasedla. O pojavu so nemudoma obvestili uporabnike Klika s posebnim obvestilom po elektronski pošti, pojasnili pa so tudi, kako ravnati v primeru, da se jim ponarejena stran prikaže, pojasnjuje Strojanova.

Z odkrivanjem storilca se ukvarjajo organi pregona, saj gre za sum storitve kaznivega dejanja. Z e-zlorabami se ukvarjajo specialisti, t.i. računalniški forenziki.

Kako prepoznati ponarejeno stran?

Ponarejeno vstopno stran Klika prepoznate tako, da se na zaslonu ne izpišeta ime in priimek uporabnika Klika, na strani ni varnostnega

Uvod v revidiranje - primeri

Namen / cilji

vir: internet (Google – slike)

Uvod v revidiranje - primeri

Pregled dokumentacije

vir: internet (Google – slike)

Uvod v revidiranje - primeri

Aktivnosti

vir: internet (Google – slike)

Uvod v revidiranje - primeri

Izvajanje

vir: internet (Google – slike)

Uvod v revidiranje - primeri

Razgovori

Vir: internet (Google – slike)

Uvod v revidiranje - primeri

Realizacija ciljev

vir: internet (Google – slike)

Uvod v revidiranje - primeri

Uvod v revidiranje – terminologija

SSKJ: „revizija“

- pregled poslovanja, dokumentov zaradi ugotavljanja skladnosti s predpisi, zakoni
- pregled kakega dokumenta, besedila, da se ugotovi pravilnost, ustreznost

Uvod v revidiranje – terminologija

iSlovar: „revizija“

- preverjanje delovanja funkcije, procesa

iSlovar: „revizija informacijskih sistemov“

- posel revidiranja, katerega namen je z izbranimi sodili opredeliti pravilnost sistema ter oblikovati načine za preprečevanje in odpravljanje nepravilnosti
- posel revidiranja, katerega namen je presoditi pravilnost tehnične odprtosti in usmerjenosti informacijskega sistema

Uvod v revidiranje – terminologija

Definicija:

- Revizija informacijskega sistema je postopek pregleda širšega okolja informacijskega sistema z namenom izdaje ustreznega zagotovila o delovanju in/ali skladnosti z zakonodajo, standardi, pravili in načeli stroke.

Zaključek / povzetek

Pridobili ste informacije o:

- Predavatelju
- Asistentki
- Predmetu
- Načinu dela
- Komunikaciji
- Izpitu
- Uvod v revidiranje

Za konec

- Pripombe
- Komentarji
- Predlogi