SIGURNOST RAČUNARSKIH MREŽA (SRM)

Tema 15:

Planiranje održanja kontinuiteta posla i oporavka od nesreća

URLs:

- Zvanična Web strana: www.viser.edu.rs/predmeti.php?id=122
- Dodatni resursi: www.conwex.info/draganp/teaching.html
- Knjige:

  www.conwex.info/draganp/books.html
- Teme za seminarske radove:

  www.conwex.info/draganp/SRM_seminarski_radovi.html

Napomena

- Ovo je skraćena verzija prezentacije / predavanja na temu **“Planiranje održanja kontinuiteta posla i oporavka od nesreća”**

Planiranje održanja kontinuiteta posla i oporavka od nesreća

- Sadržaj poglavlja i predavanja:
  - 15.1 Planiranje održanja kontinuiteta posla
  - 15.2 Planiranje oporavka od nesreće
  - 15.3 Rezervne kopije podataka
  - 15.4 Forenzička analiza

Quote

"Just because the river is quiet does not mean the crocodiles have left."

– Malay proverb

Potrebna predznanja

- Programiranje
- Za primenu:
  - Računarske mreže i protokoli
  - Operativni sistemi
  - Sistemsko programiranje
  - Strukture i modeli podataka, baze podataka

BC i DR Planning

- Business Continuity and Disaster recovery planning are processes that help organizations prepare for disruptive events
- Business Continuity and Disaster recovery refers to an organization's ability to recover from a unexpected event and/or disaster and resume or continue operations. Organizations should have a plan in place (usually referred to as a „Business Continuity Plan" or „Disaster Recovery Plan") that outlines how this will be accomplished. The key to successful disaster recovery is to have a plan (emergency plan, disaster recovery plan, continuity plan) well before disaster ever strikes.

Planiranje održanja kontinuiteta posla

- Planiranje održanja kontinuiteta posla (engl. *Business Continuity Planning*)
  - Sposobnost organizacije da se oporavi od nesreće ili neočekivanog remetilačkog događaja i nastavi rad.
  - Planiranje i stvaranje strukture koja će obezbediti nastavak posla u slučaju nesreće ili remetilačkog događaja
    - pripremu i testiranje radnji neophodnih za zaštitu ključnih poslovnih procesa od posledica velikih sistemskih i mrežnih kvarova.
  - Odnosi se na sve važne oblasti obrade informacija u kompaniji, što recimo uključuje, ali nije ograničeno na:
    - servere, *storage* sisteme
    - telekomunikacione veze i veze za prenos podataka
    - najbitnije radne stanice, prostor za rad, aplikacije i podatke
    - proizvodne i poslovne procese.

Planiranje održanja kontinuiteta posla…

- Remetilački događaj
  - bilo koja namerna ili nenamerna povreda sigurnosti kojom se obustavlja tok normalnih operacija
    - prirodno izazvani (viša sila):
      - požari, eksplozije, ili izlivanje materija opasnih po okolinu,
      - zemljotresi, oluje, poplave i požari usled prirodnih nepogoda,
      - nestanci struje ili drugi kvarovi.
    - koje izazivaju ljudi
      - podmetanje bombi, sabotaža ili drugi namerni napadi,
      - štrajkovi i druge poslovne aktivnosti,
      - nedostupnost zaposlenih ili operatera zbog hitne evakuacije
      - kvarovi komunikacione infrastrukture ili zastoji nastali njenim ispitivanjem.

Standard BS 25999

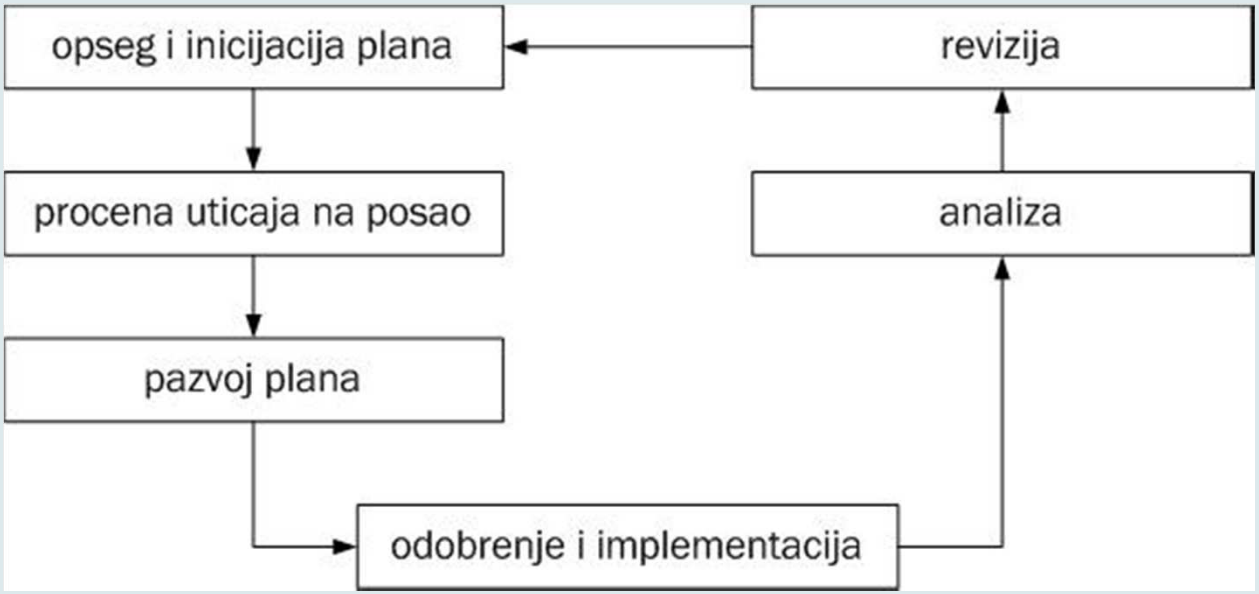
- British Standards Institution (BSI), BS 25999
- Produced by the British Standards Institution (BSI), BS 25999 is a Business Continuity Management (BCM) standard in two parts.
  - "BS 25999-1:2006 Business Continuity Management. Code of Practice", takes the form of general guidance and seeks to establish processes, principles and terminology for Business Continuity Management.
  - "BS 25999-2:2007 Specification for Business Continuity Management", specifies requirements for implementing, operating and improving a documented Business Continuity Management System (BCMS), describing only requirements that can be objectively and independently audited.

Standard ISO/IEC 27031:2011

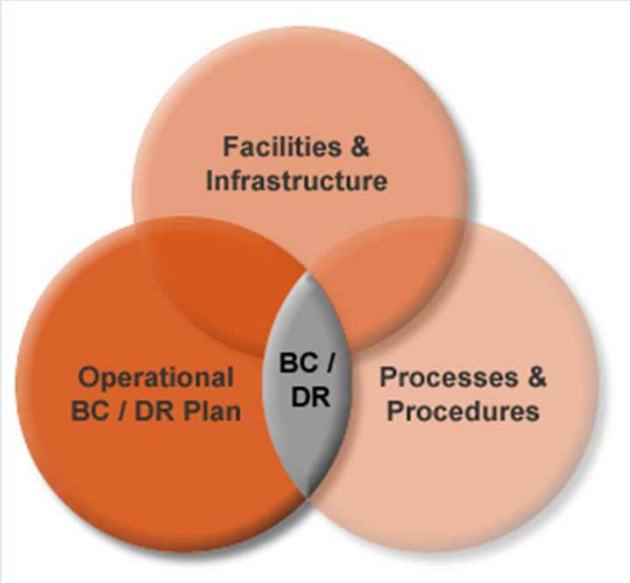
- ISO/IEC 27031:2011 - Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity
  - Abstract :
    - ISO/IEC 27031:2011 describes the concepts and principles of information and communication technology (ICT) readiness for business continuity, and provides a framework of methods and processes to identify and specify all aspects (such as performance criteria, design, and implementation) for improving an organization's ICT readiness to ensure business continuity. It applies to any organization (private, governmental, and non-governmental, irrespective of size) developing its ICT readiness for business continuity program (IRBC), and requiring its ICT services/infrastructures to be ready to support business operations in the event of emerging events and incidents, and related disruptions, that could affect continuity (including security) of critical business functions. It also enables an organization to measure performance parameters that correlate to its IRBC in a consistent and recognized manner.
    - The scope of ISO/IEC 27031:2011 encompasses all events and incidents (including security related) that could have an impact on ICT infrastructure and systems. It includes and extends the practices of information security incident handling and management and ICT readiness planning and services.

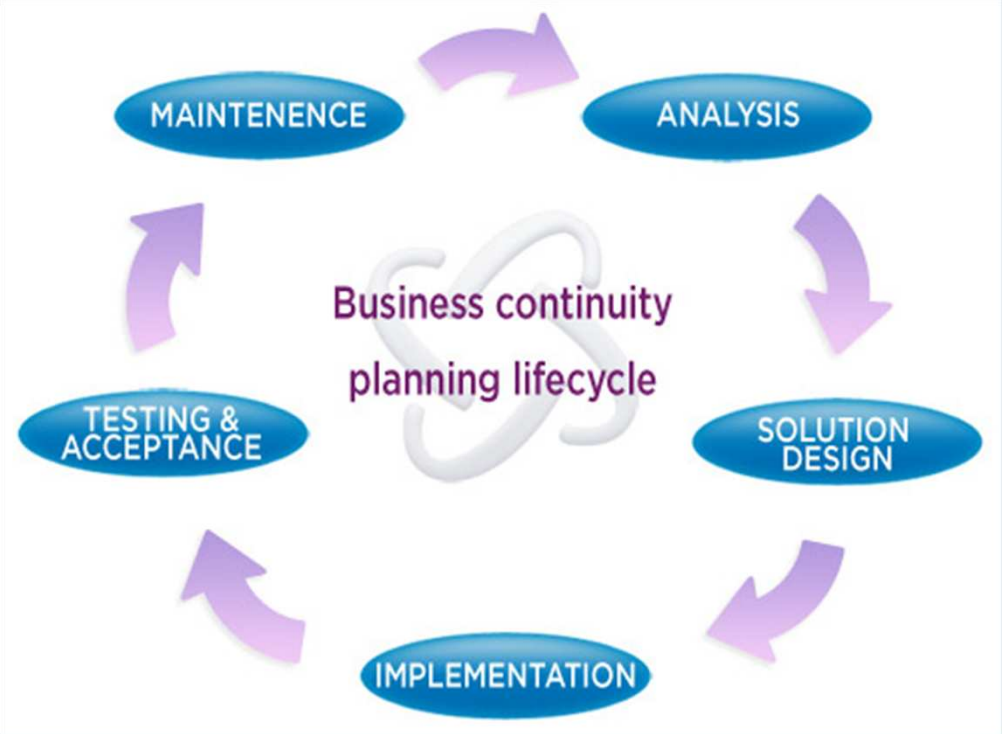
Planiranje održanja kontinuiteta posla

- Životni ciklus procesa planiranja kontinuiteta posla



Planiranje održanja kontinuiteta posla...





Planiranje oporavka od nesreće

- Planiranje oporavka od nesreće (engl. *Disaster Recovery Planning*)
- Omogućavanje implementacije važnih procesa na drugom (rezervnom) mestu, i vraćanje na prvobitno mesto i obradu u što kraćem vremenskom okviru.
- Više načina:
  - recipročna pomoć
  - vrelo, toplo i hladno mesto
  - više centara

Planiranje oporavka od nesreće

- Uzajamna (recipročna) pomoć
  - obe strane se dogovaraju da podržavaju jedna drugu u slučaju remetilačkog događaja.
  - sporazum se pravi na bazi pretpostavke da će svaka od organizacija članica sporazuma, biti u mogućnosti da podrži onu drugu u trenutku kada se ukaže potreba
  - druga kompanija treba da ima slične hardverske ili softverske konfiguracije, komunikacionu infrastrukturu kao i vaša organizacija.

Planiranje oporavka od nesreće…

- Vrelo mesto (engl. *hot site*)
  - "The very best of" tj. najbolje rešenje, ali ima veliku cenu
    - potpuno konfigurisana kompjuterizovana lokacija sa sopstvenim napajanjem, HVAC (Heating, Ventilating, and Air Conditioning), i funkcionalnim serverima datoteka / štampača i radnim stanicama.
    - Aplikacije su instalirane su na serverima i radnim stanicama i redovno se ažuriraju da bi imitirali produkcioni sistem.
  - Teoretski, osoblje može da ušeta, odradi zadnji *restore* sa inkrementalnog backupa i započe normalne operacije za veoma kratko vreme.

Planiranje oporavka od nesreće…

- Hladno mesto (engl. *cold site*)
  - najmanje spremno od sve tri opcije
  - verovatno se najčešće koristi (prvenstveno zbog niske cene).
    - soba sa napajanjem i HVAC-om
    - na mestu ne postoji nikakav kompjuterski hardver
    - spremno je za unos računarske opreme u vanrednoj situaciji
    - aplikacije će morati da budu instalirane i tekući podaci vraćeni sa rezrevnih kopija

Planiranje oporavka od nesreće…

- Toplo mesto (engl. *warm site*)
  - Zlatna sredina
    - kompjuterizovana lokacija, sa sopstvenim napajanjem i HVAC,
    - Može imati servere datoteka / štampača, ali ne i čitav skup radnih stanica
    - Aplikacije nisu instalirane
  - Da bi se na ovom tipu mesta omogućila udaljena obrada, radne stanice će morati da budu isporučene brzo, a aplikacije i njihovi podaci moraće da se vrate sa rezervnih kopija.

Arhiviranje i rezervne kopije

- Arhiviranje i *backup* su veoma značajni
  - neophodno za oba procesa
  - arhiviranje – podaci korisnika radnih stanica
    - dužnost zaposlenih, tj. korisnika
  - backup – OS, mreža (npr. *Active Directory*), aplikacije od značaja, servisi, podaci
    - dužnost administratora
  - Softver
    - Linux – dosta besplatnih alata. U krajnjem slučaju, `tar` i `cpio` + `cron` mogu sasvim korisno poslužiti.
    - Windows – ima komercijalnih i besplatnih alata, kao i alata koji su sastavni deo operativnog sistema.

Računarska forenzička analiza

- Sigurnost kao proces:
  - Procena
  - Zaštita
  - Otkrivanje
  - Odgovor
    - "zakrpi i nastavi" ili
    - "goni i sudi"

- Odgovor "goni i sudi" zahteva primenu forenzičke analize za prikupljanje dokaza.

Računarska forenzička analiza

- Razlikuje se od klasične forenzičke analize
- Digitalni dokazi mnogo ranjiviji od fizičkih
  - veštom napadaču mnogo lakše da ukloni tragove svog delovanja
  - nepažljivo ili nestručno sprovođenje istrage takođe može rezultirati gubitkom ključnih podataka
  - za utvrđivanje postojanja dokaza potrebno je sprovesti sveobuhvatnu analizu računarskog sistema i mreže.

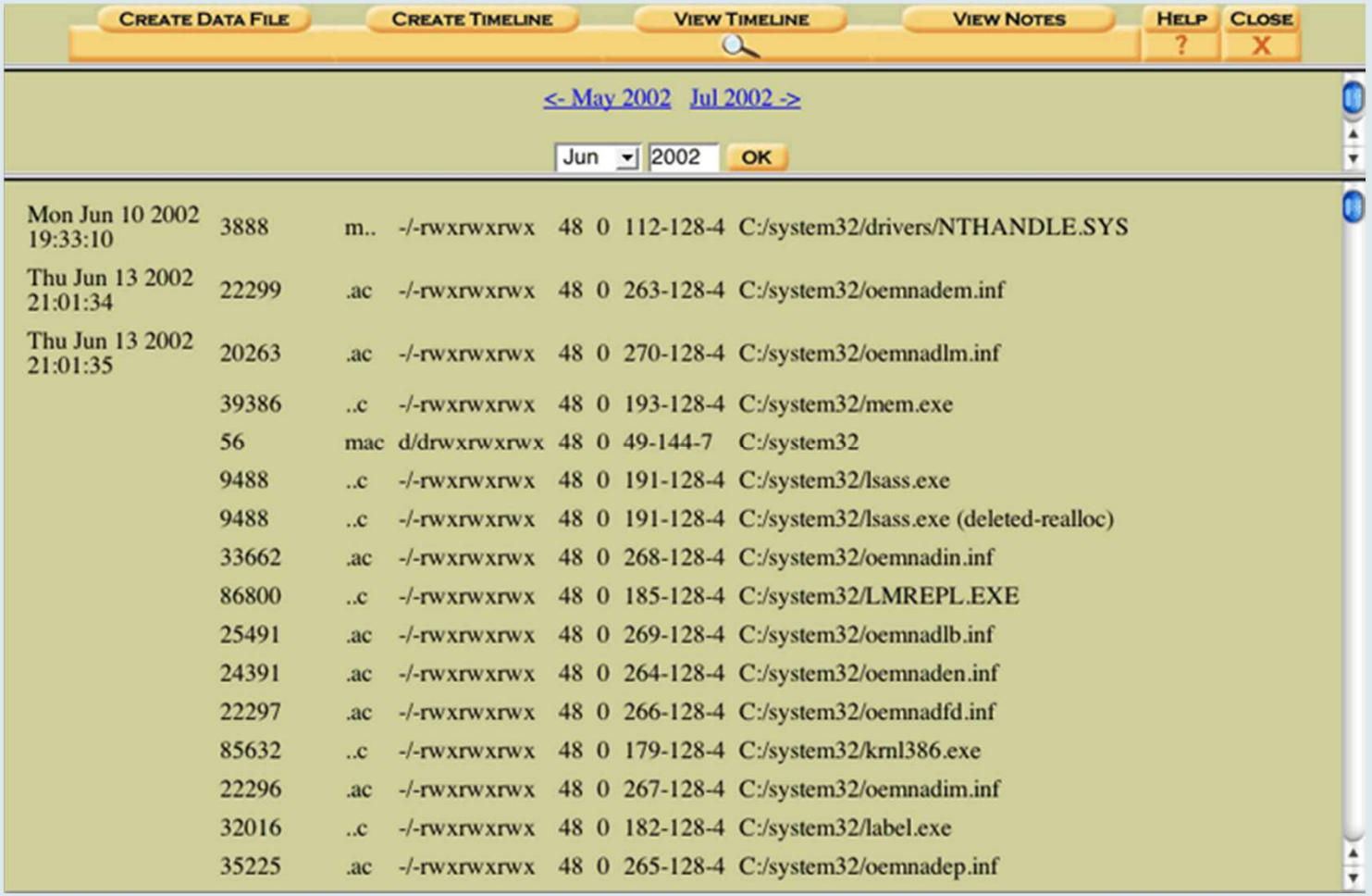
Računarska forenzička analiza…

- Proces forenzičke analize
  - Prikupljanje podataka i dokaza
    - live system acquisition – memory dump
      - npr. linux: pregledati fajlove `/dev/mem` i `/proc/kcore`
    - disk data acquisition
      - npr. windows: recycle bin, registry, temp, sys.vol.info
    - decryption / cryptanalysis
  - Analiza dokaznih materijala
    - Analiza vremenskog redosleda događaja
    - Analiza skrivenih podataka
    - Analiza aplikacija i datoteka
    - Analiza vlasništva

Računarska forenzička analiza...

- Forenzički alati
  - The Sleuth Kit / Autopsy Browser
    - analiza sadrža direktorijuma, uključujući i izbrisane datoteke,
    - analiza sadržaja datoteka (u ASCII ili hex formatu, moguća ekstrakcija delova datoteka),
    - praćenje vremenskog redosleda događaja na osnovu vremena pristupa i izmene objekata,
    - pretraživanje sadržaja na osnovu regularnih izraza,
    - analiza metapodataka u sistemu datoteka, itd.

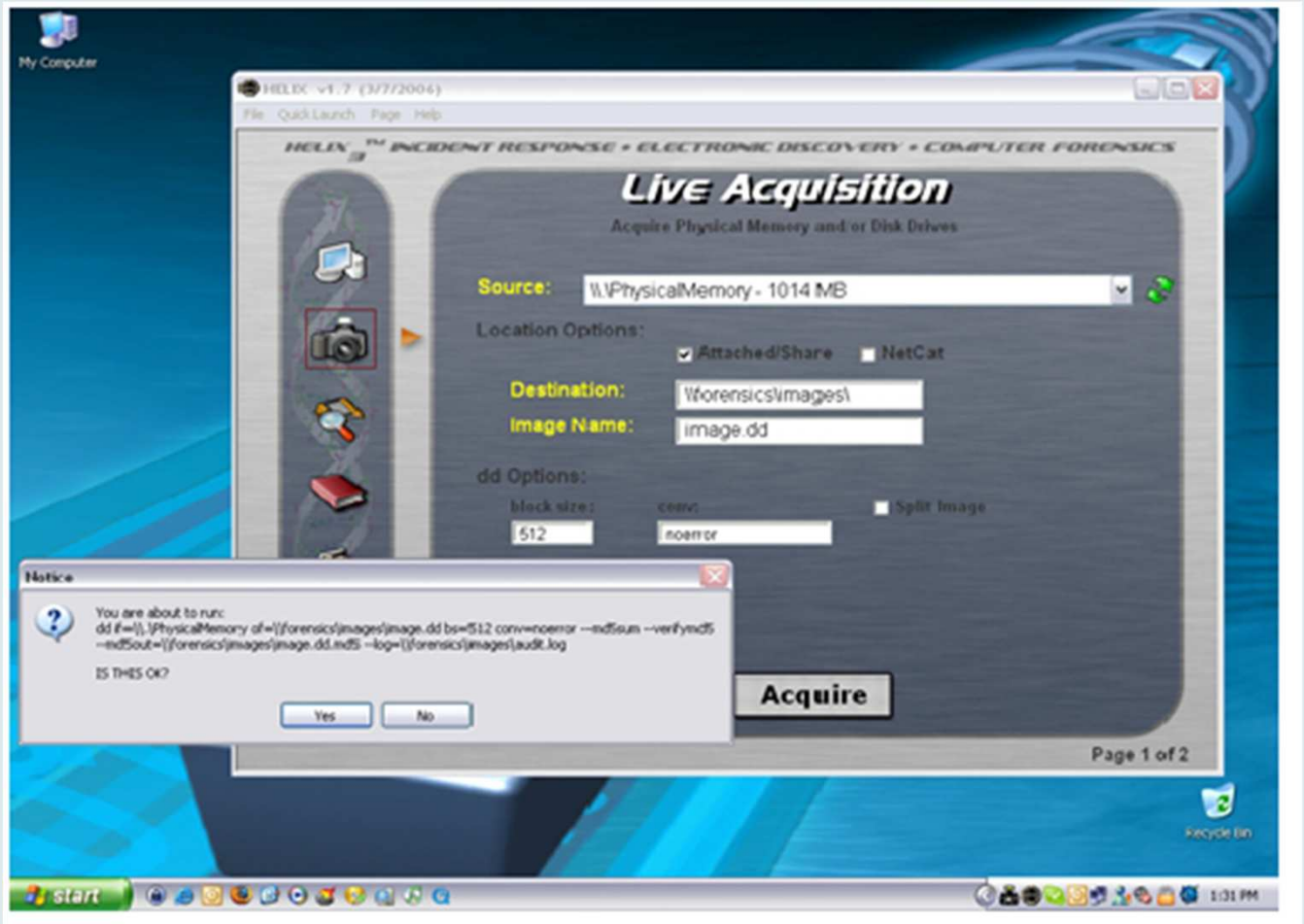
TSK



Računarska forenzička analiza...

- Forenzički alati
  - Helix CD
    - varijacija Knoppixa prilagođena forenzici
    - Podiže se sa CD-a, ne ostavlja tragove niti obavlja bilo kakve izmene na sistemu koji se analizira (što se i očekuje od ozbiljnog forenzičkog alata)
    - sadrži gomilu forenzičkih alata uključujući TSK
    - omogućava Live Acquisition na Windows sistemima
    - ono što je BackTrack za pen.test, to je Helix za forenzičar
    - www.e-fense.com/helix/

Helix



Literatura

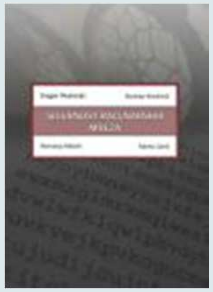
- D. Pleskonjić, N. Maček, B. Đorđević, M. Carić: **"Sigurnost računarskih sistema i mreža"**, Mikro knjiga, Beograd, 2007., ISBN: 978-86-7555-305-2, knjiga – udžbenik
- www.conwex.info/draganp/books_SRSiM.html
- www.mikroknjiga.rs/store/prikaz.php?ref=978-86-7555-305-2

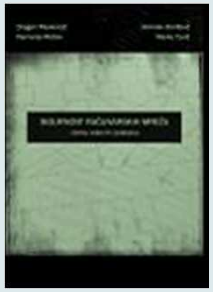
- Za predavanje 15:
  - Poglavlje 15: Planiranje održanja kontinuiteta posla i oporavka od nesreća

Literatura - nastavak

- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **"Sigurnost računarskih mreža"**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-16-5, knjiga - udžbenik
- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **"Sigurnost računarskih mreža - priručnik za laboratorijske vežbe"**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-49-1
- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **"Sigurnost računarskih mreža - zbirka rešenih zadataka"**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-55-6

www.conwex.info/draganp/books.html





Dodatna literatura

- **Applied Cryptography**
  Bruce Schneier
  John Wiley & Sons, 1995

- **Cryptography and Network Security**
  William Stallings
  Prentice Hall, 1998

- **The CISSP Prep Guide – Mastering the Ten Domains of Computer Security**
  Ronald L. Krutz, Russell Dean Vines
  John Wiley & Sons, 2001

  Druge knjige i razni *online* resursi

- ***Napomena:*** tokom predavanja će biti naglašena dodatna literatura, po potrebi.

Pitanja

?