integrirana sigurnost

BAZE PODATAKA I RAČUNALNA FORENZIKA

Damir Delija
Dr.Sc.E.E

Plan predavanja

- Cilj prezentacije
  - dati pregled što je računalna forenzika i kakvo je stanje za baze podataka
- Proći će se kroz
  - što je računalna forenzika i specifičnosti na području baza podataka
  - reakcije na incidente i računalna forenzika
  - alati, komercijalni i open source
  - primjene i uvođenja alata u postojeće velike sustave

Razvoj računalne forenzike

Dva osnovna motiva

- razvoj računalnih znanosti i
- razvoj računalnih incidenata tj užem smislu računalni kriminal

integrirana sigurnost

Računalna forenzika

“Computer Forensics is simply the application of computer investigation and analysis techniques in the interest of determining potential legal evidence"

Judd Robbins

Zahtjevi na postupak računalne forenzike

- Postupak mora biti dobro dokumentiran i rezultati moraju biti ponovljivi
- Princip "najbolji dokazni materijal" tj. analiza se radi na egzaktnoj kopiji a ne živom sustavu
- Lanac kontrole dokaza (Chain of custody) mora garantirati pouzdanost dokaza

Legalni kriteriji

Uspostavljeni su slučaju Daubert/Frye:

- Da li je tehnika i postupak pouzdano testiran;
- Da li je tehnika i postupak objavljen, provjeren od znanstvene zajednice;
- Da li se pouzdano zna koja je vjerojatnost greške tehnike ili postupka;
- Da li je tehnika i postupak prihvaćena od znanstvene zajednice.

Koraci forenzičkog postupka

Priprema

- priprema alata i opreme potrebne za forenzički postupak;

Prikupljanje

- prikupljanje dokumenta, logova, datoteka i izrada kopija fizičkih objekata koji sadrže elektroničke dokaze

Ispitivanje dokaza

- izdvajanje dokaza iz prikupljenog materijala

Analiza

- analiza dokaza prikupljenih u koraku ispitivanja dokaza

Izvještavanje

- izrada izvještaja o nalazima

integrirana sigurnost

Računalna forenzika - obzirom na obuhvat sustava

Forenzika pojedinačnog računala (host based)

- najčešći slučaj - analize radne stanice
- ulazi i forenzika aplikacije

Mrežnu forenziku (network enabled),

- analizu sustava na razini mreže, analizu prometa na mreži, upravljanja mrežom

Forenzika logova sustava (system log forensic)

Specifičnosti forenzike poslužitelja baza podatka i baza podataka

Sličnosti:

- forenzičke metode koje se koriste su iste kao i za druge složene računalne sustave

Razlike:

- zahtjevi maksimalne raspoloživosti sustava,
- veliki volumen podataka,
- visoka pouzdanosti podataka,
- neprihvatljivosti zaustavljanja sustava
- ograničena ekspertiza raspoloživa u trenutku incidenta

integrirana sigurnost

Dodatne specifičnosti forenzike sustava baza podataka

Način na koji se dolazi do pokretanja forenzičkog postupka (otkrića incidenta)

- većina „data breach“ incidenata otkriva se naknadno i izvana
- otežano otkrivanje tragova i vektora ulaska

integrirana sigurnost

Standardni koraci računalne forenzike za baze podataka

- Pokretanje dokumentiranog opisa događaja u sustavu
- Identificiranje i kontrola incidenta
- Izrada i pohrana datoteka sa elektroničkim dokazima u lancu odgovornosti o dokazima
- Oporavak usluga i vraćanje / rekonstrukcija obrisanih podataka
- Prikupljanje i klasificiranje metadata podataka po vremenu
- Povezivanje svih informacija o događajima u lanac događaja na osnovi vremena
- Analiza metadata timelinea
- Dokumentiranje cijelog forenzičkog procesa
- Korištenje rezultata u daljim koracima
- Detaljna analiza ključnih podatka

Računalna forenzika - po pristupu

Proaktivna računalna forenzika

- primjeni metoda računalne forenzike na zdravom sustavu kako za dobivanje baseline sustava.

Retroaktivna računalna forenzika (klasična forenzika)

- Primjena i bez proaktivne ali puno manja efikasnost

Preduvjet za forenziku je kvalitetna administracija sustava

integrirana sigurnost

Rezultat forenzičkog postupka završno izvješće o incidentu

- Završno izvješće incidentu

  sadrži relevantne podatke o incidentu;

  glavni cilj - podizanje razine sigurnosti;

  informacije iz tog izvješća moraju omogućiti:

  - prepoznavanje izvora napada;
  - prepoznavanja i uklanjanje sigurnosnih propusta

- Koristiti se u sklopu procesa za upravljanje sigurnosnim incidentima

- Računalna forenzika kao dio procesa kontrole incidenata i kao dio procesa nadzora sustava

Alati i ekspertiza

Ne postoje namjesnki alat za forenziku baza

- Postoje alati za forenziku računalnog sustava na nivou operacijskog sustava i sklopovlja
- Ne postoje alati forenziku baze podataka i pripadne aplikacije
- Ekspertiza vrlo rijetka

Komercijalni alati ili Opensource

- Nema idelanog alata
  - može postojati zahtjevani alat!
- Prednost sa pravne strane na Komercijalnim alatima
- Opensource dodatni / kontrolni
- Filozofija odabira ista kao i za druge korporativne sustave
  - ključno je što mislite raditi i kako u vašem sustavu
- Na samim bazama – open source ili home made dominiraju

integrirana sigurnost

Alati

- EnCase guidance software
- FTK
- Helix CD
- The Coroner's Toolkit (TCT)
- logminer
- Mnogi drugi

integrirana sigurnost

Primjene i uvođenja alata u postojeće sustave

- Primjene i uvođenja alata u postojeće velike sustave
  - dio incident responsa (IR)
  - dio preventivne pripreme
- Samo novi pogleda na stare prokušane tehnike kontrole sustava
  - dobra administracija sustva
- Dio pripreme za nastavak poslovanja
  - bitno razumjevanje važnosti

Zaključak

- Računalna forenzika je dio kontrole i oporavka od incidenta
  - prepoznavanje mogućnosti računalne forenzike
- U dogledno vrijeme možemo očekivati sve veću pojavu i objavljivanje incidenata
- incidenti se ne mogu više držati unutar kuće
- incidenati moraju biti legalno ispravno odrađeni
- Korištenje metoda računalne forenzike mora biti sustavno i kao takvo ugrađeno u organizaciju
- Potrebna znanja i postupci moraju biti prepoznati kao nešto što se mora imati na raspolaganju

Bez takvog pristupa računalni sustavi su izuzetno ugroženi

Linkovi i siteovi

www.databasesecurity.com

Krovni site za forenziku baza podataka

www.databasesecurity.com/oracle-forensics.htm

Oracle forenzika

www.sans.org/reading_room

Različiti aspekti računalne sigurnosti

http://forensics.sans.org/community/downloads/

"SANS Computer forensic and E-Discovery"
SANS portal za računalnu forenziku

integrirana sigurnost

Pitanja ?

damir.delija@insig2.hr

www.insig2.hr