LOGGING I MONITORING

Informaciona bezbednost

FAKULTET TEHNIČKIH NAUKA

V7

Sadržaj

- Logging
- Prednosti generisanja log zapisa i neporečivost
- Neporečivost
- Zahtevi logging mehanizma
- Kvalitetan log zapis
- Format log zapisa
- Skladištenje logova
- Rotacija logova
- Pristup logovima
- GoLang vs Java

LOGGING

Logging treba da obezbedi da svaka neuspešna prijava, svi nevalidni podaci, koji su stigli na server, i ostale sumnjive situacije, budu zabeležene. Na taj način će se omogući blagovremeno identifikovanje malicioznih naloga i različitih napada na sistem.

LOGGING

Primeri događaja koji treba da se loguju:

- Greške (errors) koje su se dogodile;
- Promena konfiguracije;
- Skladištenje i dobavljanje podataka;
- Korisnički zahtevi i odgovori sistema;
- Kontrola pristupa itd.
- Događaji relevantni za bezbednost - Primeri?

LOGGING

Primeri događaja koji treba da se loguju:

- Greške (errors) koje su se dogodile;
- Promena konfiguracije;
- Skladištenje i dobavljanje podataka;
- Korisnički zahtevi i odgovori sistema;
- Kontrola pristupa itd.
- Događaji relevantni za bezbednost
  - -uspešne/neuspešne prijave na sistem
  - -neuspešna kontrola pristupa

Prednosti generisanja log zapisa i neporečivost

- Uz pomoć logginga programeri mogu da preduprede probleme i da brzo reaguju, kada se novi problem desi, što je od velikog značaja, posebno kada je sistem već u produkciji.
- Logging obezbeđuje i ulazne podatke za sisteme za monitoring.
- Kolekcije log zapisa se mogu slati alatima za monitoring, koji imaju zadatak da prate događaje u sistemu i da “okinu” alarm svaki put kada se sumnjivo ponašanje dogodi.
- Još jedan od primera primene jesu i različite forenzičke analize i istrage.
- Smernice u pogledu čuvanja log zapisa se mogu pronaći u zakonu, pravilnicima delatnosti i slično.

Neporečivost

Kada neki subjekat izvrši akciju, pogotovo ako je ona osetljive prirode, potrebno je zabeležiti informaciju da je ta akcija izvršena, u kom trenutku se to desilo, i koji subjekat je bio izvršitelj. Na ovaj način se sprečava poricanje izvršenja neke aktivnosti od strane subjekta. Primeri akcija, koje korisnik može da izvrši su:

- Promene konfiguracije;
- Kreiranje informacija;
- Slanje poruke;
- Primanje poruke i davanje različitih potvrda itd.

Zahtevi logging mehanizma

Logging mehanizam treba da bude:

- kompletan

  -dovoljno informacija da se dokaže neporečivost

- upotrebljiv

  -podržati efikasnu ekstrakciju događaja iy log yapisa

- koncizan

  -minimalna količina informacija, optimizovati zapise da sadrže minimalnu količinu memorije

Navedena 3 zahteva je moguće formalno ispuniti bez istraživanja i mnogo truda, no to rešenje neće biti kvalitetno. Da bi se date stavke ispunile neophodno je razmotriti savete i najbolje prakse koje možete pronaći online, poput onih navedenih u OWASP ASVS standardu.

Kvalitetan log zapis

Log zapisi često sadrže osetljive podatke

-Koji podaci bi bili osetljivi?

-Šta uraditi po tom pitanju?

Kvalitetan log zapis

Log zapisi često sadrže osetljive podatke

-Koji podaci bi bili osetljivi?

-Šta uraditi po tom pitanju?

- Izbegavati čuvanje osetljivih podataka, osim ako to nije neophodno
- Ako se osetljivi podaci čuvaju-zaštiti ih-šifrovati ili hešovati

Format log zapisa

Najveći problem prilikom rada sa logovima je što su, uglavnom, kreirani u nestrukturiranom formatu, što otežava efikasnu ekstrakciju korisnih informacija. Prilikom kreiranja logova treba voditi računa da format log zapisa podržava obradu, da lako može da se parsira i obradi od strane centralizovanog sistema za upravljanje logovima.

Format log zapisa

Log zapis treba da sadrži:

- **Datum** - Tačan datum kada se događaj desio.
- **Vreme** - Tačno vreme kada se događaj desio.
- **Izvor događaja** - Koji program, komponenta ili korisnički nalog je prouzrokovao događaj.
- **Tip događaja** - Da li je u pitanju error, warning, success ili neki drugi tip događaja.
- **ID događaja** - Identifikacioni broj događaja.
- **Poruka** - Poruka koja bliže opisuje konkretan događaj ili rezultat događaja.

Datum i vreme ne treba generisati u proizvoljnom formatu, već treba ispratiti neki od postojećih standarda. Preporuka je da se koristi ISO standard: ISO 8601:2004, Data elements and interchange formats – Information interchange – Representation of dates and times.

Ukoliko se sistem sastoji od više različitih uređaja, koji generišu logove, satove uređaja treba sinhronizovati sa satom glavne komponente sistema.

Logging mehanizam treba da bude implementiran tako da zaštiti integritet datuma i vremena i da detektuje svaku neautorizanu promenu.

Skladištenje logova

Svaka komponenta u sistemu treba da upravlja svojim logovima i alocira memoriju za skladištenje log zapisa. U slučaju da komponenta sistema nema adekvatnu logiku za upravljanje logovima, može da se, u određenoj meri, osloni na eksterne komponente ili na sistem u koji je integrisana. U takvim situacijama logovi mogu da se periodično šalju npr. nekom centralizovanom sistemu, koji će omogućiti njihovo dalje parsiranje, te filtriranje i pretraživanje.

Komponenta, kada je blizu da popuni svoje skladište, treba da pošalje odgovarajuće upozorenje (warning) sistemu. Administrator će, kada vidi upozorenje, dalje odlučivati koji će se koraci izvršavati ili će sistem sam automatski znati šta treba da uraditi.

Skladištenje logova

Koliko dugo treba čuvati log zapise?

1 godinu, 5 godina, 10 godina?

Koliki kapacitet za logove treba da se obezbedi?

Rotacija logova

Rotacija logova predstavlja automatizovan proces koji podrazumeva arhiviranje ili brisanje log zapisa, kada je prošao određeni vremenski period ili kada log zapisi popune predodređeni kapacitet memorije. Kada se prilikom rotacije logova obrišu/arhiviraju logovi iz log datoteke, novi logovi mogu da se upisuju u tu datoteku.

Neophodno implementirati!

Zaštita logova

- Zaštita pristupa fajlovima od neautorizovane izmene/brisanja.
- Svaki pristup je neautorizovan ukoliko ne dolazi od same aplikacije koja generiše te logove.
- Ne bi smeo bilo koji korisnik računara da pristupi log zapisima, da ih obiše ili izmeni.

- Logovi koji se mogu izmeniti ili obrisati su beskorisni
- Zaštititi logove od neautorizovane izmene ili brisanja
- Sprečiti log injection - u logovima mogu da se nađu podaci koje korisnik unosi - sanitizacija unosa
- Sistem koji proizvodi logove jedini ima pravo upisa

Neophodno implementirati!

Načini za logovanje

GoLang

- log(ugrađeno) - nije fleksibilan po pitanju formata log zapisa
- logrus
- ...

Java

- java.util.logging(ugrađeno)
- Log4j
- Slf4j