LOGGING I MONITORING

- Smernice -

Bezbednost u sistemima elektronskog poslovanja

Sadržaj

Logging i monitoring

Log zapisi koje generišu aplikacije i operativni sistemi nekog postrojenja su veoma korisni, kako sa aspekta debagovanja problema, tako i za potrebe ispitivanja bezbednosnih propusta. Log zapisi predstavljaju osnovni mehanizam za postizanje neporecivosti.

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 omogućiti blagovremeno identifikovanje malicioznih naloga i različitih napada na sistem.

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.

1. Prednosti generisanja log zapisa i neporecivost

Logging je koncept, koji se koristi od strane programera, za debagovanje i ispitivanje sistema. Uz pomoć ovog koncepta 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.

Neporecivost

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.

Na primer: Neporecivost nas štiti od situacija kada administratoru operater sistema kaže da nije izvršio promenu konfiguracije baze, a log zapis potvrđuje da je upravo taj operater bio korisnik sistema, koji je izvršio tu akciju.

2. Zahtevi *logging* mehanizma

Logging mehanizam treba da bude:

- kompletan,
- upotrebljiv i
- koncizan

Kompletnost

Log zapis mora da sadrži dovoljno informacija da dokaže neporecivost. Svaki događaj, za koji je neporecivost potrebna, treba da bude zabeležen.

Dodatno, svaki *security-related* događaj, interesantan za potrebe *monitoring*-a, treba da bude zabeležen.

Upotrebljivost

Logging mehanizam treba da podrži efikasno ekstrakciju događaja iz log zapisa.

Konciznost

Logging mehanizam treba da proizvodi najmanju količinu zapisa koji su potrebni da ispuni svoju svrhu. Dodatno, optimizovati svaki zapis da sadrži sve informacije, a zauzima najmanju 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.

3. 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.

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.

4. 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.

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.

Koliko dugo treba čuvati log zapise? 1 godinu, 5 godina, 10 godina? Koliki kapacitet za logove treba da se obezbedi? Uništavanje ili arhiviranje logova, kao i alociranje potrebnog prostora treba uskladiti sa politikom firme, domenom i prirodom sistema, kao i sa svim zakonskim regulativama.

5. Pristup logovima

Log zapisi su bitni u svakom sistemu zbog korekcije grešaka, potencijalnih istraga itd. Osim što njihovo skladištenje mora da bude bezbedno, neophodno je obezbediti kontrolu pristupa log zapisima za korisnike i/ili softverske alate razmatranog sistema. Čitanje ne sme da bude privilegija svakog korisnika, već samo određenih subjekata sistema, kao što je npr. administrator. Sistem koji proizvodi logove je jedini subjekat koji ima prava pisanja u log datoteke.

Log zapisi ne smeju da se menjaju ili brišu, te se osim neautorizovanog pristupa, treba zaštititi i od neautorizovane izmene i brisanja. Ukoliko prava pristupa log datoteci nisu konfigurisana, administrator, koji ima pristup *file* sistemu, bi mogao da izmeni ili obriše tu datoteku.