POSLOVNA SOFTVERSKA OS REŠENJA

školska 2024/2025 godina

Vežba 11: Sigurnost podataka u poslovnim OS rešenjima

U poslovnim operativnim sistemima (OS) čuvaju se podaci koji su krucijalni za rad organizacije, a to uključuje informacije o zaposlenima, klijentima, finansijskim transakcijama, poslovnim procesima i intelektualnoj svojini. Gubitak ili kompromitacija ovih podataka može prouzrokovati velike finansijske štete, narušavanje poverenja korisnika, pravne probleme i ugrožavanje reputacije.

1. Tri osnovna principa sigurnosti podataka

- **Poverljivost (Confidentiality):** Podaci moraju biti dostupni samo ovlašćenim korisnicima, što se postiže enkripcijom i kontrolom pristupa.
- **Integritet (Integrity):** Podaci ne smeju biti neovlašćeno menjani ili oštećeni, a za to se koriste digitalni potpisi i hash funkcije.
- **Dostupnost (Availability):** Ovlašćeni korisnici moraju imati pristup podacima kada su im potrebni, što podrazumeva zaštitu od prekida rada i planove za oporavak sistema.

2. Bezbednosni izazovi u poslovnim OS

- **Napadi izvana:** Hakerski napadi, malveri kao što su virusi i ransomware, kao i DDoS napadi koji mogu onesposobiti sisteme.
- **Unutrašnje pretnje:** Nepravilna upotreba podataka od strane zaposlenih ili nenamerne greške koje mogu ugroziti bezbednost.
- **Neadekvatna zaštita:** Slabe lozinke, zastareli softver i loša konfiguracija omogućavaju lakši pristup napadačima.
- **Pravni zahtevi:** Nepoštovanje propisa poput GDPR može rezultirati visokim kaznama i gubitkom poverenja korisnika.

3. Tehnologije i alati za zaštitu podataka

3.1 Enkripcija (šifrovanje)

Šta je enkripcija?

Enkripcija je ključni mehanizam za zaštitu podataka, posebno u poslovnim operativnim sistemima gde se obrađuju osetljive informacije. Bez pravilne enkripcije, podaci su ranjivi na presretanje i zloupotrebu tokom prenosa ili skladištenja. Moderni algoritmi kao što su AES i RSA osiguravaju visok nivo sigurnosti, ali je neophodno pravilno upravljanje ključevima kako bi se sprečile potencijalne ranjivosti.

Vrste enkripcije:

- **Simetrična enkripcija:** Koristi isti ključ za šifrovanje i dešifrovanje (npr. AES). Brza je i efikasna, ali zahteva siguran način razmene ključeva.
- **Asimetrična enkripcija:** Koristi par ključeva – javni ključ za šifrovanje i privatni za dešifrovanje (npr. RSA). Omogućava sigurnu razmenu ključeva i digitalne potpise.

Upotreba u poslovnim OS:

- Šifrovanje fajlova i baza podataka da bi se sprečio neovlašćeni pristup.
- Sigurna komunikacija (npr. VPN, HTTPS).

3.2 Autentifikacija i autorizacija

Autentifikacija

Autentifikacija predstavlja proces potvrde identiteta korisnika ili sistema pre nego što im se dozvoli pristup resursima poslovnog operativnog sistema. Najčešće metode autentifikacije uključuju:

- **Lozinke** (najčešći metod, ali sa rizikom od krađe ili slabe sigurnosti).
- **Dvofaktorska autentifikacija (2FA):** Kombinuje nešto što korisnik zna (lozinka) i nešto što poseduje (telefon, token).
- **Biometrija:** Prepoznavanje lica, otisak prsta, glas. Visoko sigurnosna, ali zahteva dodatne uređaje.

Autorizacija

Nakon uspešne autentifikacije sledi **autorizacija**, koja određuje koje resurse korisnik može koristiti i koje akcije sme da izvrši. U poslovnim sistemima se često koristi model pristupa po ulogama, poznat kao **Role-Based Access Control (RBAC)**. Ovaj model omogućava dodeljivanje pristupnih prava u skladu sa poslovnom ulogom korisnika, čime se smanjuje rizik od slučajnog ili namernog pristupa osetljivim informacijama. RBAC takođe olakšava praćenje i reviziju pristupa.

3.3 Sigurnosni protokoli: SSL/TLS

- **SSL (Secure Sockets Layer)** i **TLS (Transport Layer Security)** su protokoli koji omogućavaju sigurnu komunikaciju preko mreže.
- Koriste enkripciju za zaštitu podataka između web pregledača i servera.
- Proveravaju identitet servera pomoću digitalnih sertifikata (npr. sertifikati izdat od strane CA - Certificate Authority).
- Kada vidite u pretraživaču adresu sa **https://** to znači da je SSL/TLS aktivan.

3.4 Regulative i pravni aspekti: GDPR

GDPR (**General Data Protection Regulation**) predstavlja ključnu evropsku regulativu koja postavlja standarde za zaštitu ličnih podataka i privatnost korisnika. Organizacije koje posluju u EU ili sa podacima građana EU moraju se strogo pridržavati sledećih zahteva:

- Jasno dobijanje **dozvole korisnika** za prikupljanje i obradu njihovih podataka.
- Omogućavanje prava korisnicima da pristupe svojim podacima, isprave ih ili zahtevaju njihovo brisanje, što je poznato kao **„pravo na zaborav“**.
- Obaveza pravovremenog **obaveštavanja o eventualnim povredama podataka** koje mogu ugroziti korisnike.
- Implementacija odgovarajućih **tehničkih i organizacionih mera** za zaštitu podataka, uključujući enkripciju, kontrolu pristupa i sigurnosne protokole.

Nepoštovanje GDPR-a može dovesti do značajnih novčanih kazni, ali i do gubitka reputacije i poverenja klijenata, što dodatno ističe važnost ove regulative u poslovnim operativnim sistemima. Zbog toga, kompanije moraju kontinuirano ulagati u bezbednosne mere i edukaciju zaposlenih kako bi osigurale usklađenost i zaštitile podatke svojih korisnika.

4. Upotreba veštačke inteligencije u bezbednosti

4.1 Detekcija pretnji pomoću AI

- AI sistemi koriste tehnike mašinskog učenja da analiziraju obrasce ponašanja korisnika, mrežnog saobraćaja i sistema.
- Prepoznavanje anomalija — detektuju neuobičajene aktivnosti koje mogu ukazivati na napad, poput pokušaja upada, malicioznih veza, ili širenja malware-a.
- AI može brzo analizirati velike količine podataka u realnom vremenu, što je teško ljudima.
- Koristeći modele dubokog učenja i neuronske mreže, AI može prepoznati i sofisticirane napade koji se često maskiraju kao legitimne aktivnosti.
- AI omogućava proaktivno otkrivanje novih pretnji, čak i pre nego što su poznate tradicionalnim antivirusnim programima.

4.2 Prevencija i automatska reakcija

- Sistemi mogu automatski blokirati pristup ili zahteve koji izgledaju sumnjivo.
- AI može davati preporuke za poboljšanje sigurnosti ili predviđati potencijalne napade na osnovu istorijskih podataka.
- Primer: automatsko zaključavanje naloga posle više neuspelih pokušaja prijave.
- Automatska segmentacija mreže i izolacija kompromitovanih uređaja može sprečiti širenje napada unutar poslovne mreže.

5. Najbolje prakse za bezbednost u poslovnim OS

- Redovno ažuriranje i zakrpe softvera i operativnog sistema.
- Korisnička edukacija o bezbednosnim rizicima (phishing, socijalni inženjering).
- Implementacija slojevitih sigurnosnih mera (defense in depth).
- Upotreba sigurnosnih alata za nadzor i prijavu incidenata.
- Pridržavanje zakonskih okvira i industrijskih standarda.
- Kontrola pristupa na osnovu principa najmanjih privilegija (least privilege) kako bi korisnici imali samo neophodne dozvole.
- Redovni bezbednosni auditi i testiranja ranjivosti radi identifikacije i uklanjanja slabosti u sistemu.
- Korišćenje enkripcije podataka u mirovanju i u tranzitu radi dodatne zaštite.

Primer praktične primene: Sigurnost podataka u poslovnoj aplikaciji za upravljanje korisničkim podacima

---

Zamislimo firmu koja razvija poslovnu aplikaciju za upravljanje korisničkim podacima i pružanje usluga klijentima putem web portala i mobilne aplikacije. Aplikacija sadrži lične podatke korisnika (ime, prezime, kontakt, adresa), finansijske podatke (kartice, fakture), kao i poslovne informacije.

---

1. Zaštita podataka u skladištu (data-at-rest)

Enkripcija baze podataka

- Svi osetljivi podaci u bazi (kao što su lozinke, brojevi kartica, lični identifikatori) se čuvaju u šifrovanom obliku koristeći **AES-256** algoritam.
- Lozinke se dodatno čuvaju kao **hash vrednosti** sa solju, koristeći algoritme kao što su **bcrypt** ili **Argon2**, da bi se sprečilo njihovo lako otkrivanje čak i ako baza bude kompromitovana.

Kontrola pristupa bazi

- Pristup bazi podataka je ograničen samo na određene aplikacijske servere i servise, preko **VPN** mreže i sa specifičnim pristupnim pravima.
- Koriste se **principi najmanjih privilegija** (Least Privilege), gde korisnici i servisi dobijaju samo neophodne dozvole.

---

2. Zaštita podataka u prenosu (data-in-transit)

Sigurna komunikacija

- Sve komunikacije između korisničkog uređaja i serverske aplikacije se odvijaju preko **HTTPS** protokola, koji koristi **TLS 1.2 ili TLS 1.3** za enkripciju podataka u mreži.
- Time se sprečava presretanje i manipulacija podacima od strane trećih strana (npr. na javnim Wi-Fi mrežama).

Digitalni sertifikati

- Server poseduje validan **SSL/TLS sertifikat** izdat od strane CA (Certificate Authority).
- Sertifikati se redovno ažuriraju i proveravaju da ne bi došlo do kompromitacije.

---

3. Autentifikacija i autorizacija korisnika

Višefaktorska autentifikacija (MFA)

- Prilikom prijave, korisnik unosi lozinku, a zatim prima jednokratni kod (OTP) putem SMS-a ili generisan u aplikaciji (Google Authenticator).
- Ovo značajno smanjuje rizik od neovlašćenog pristupa čak i ako je lozinka kompromitovana.

Upravljanje pristupnim pravima

- Korisnici se kategorizuju u grupe sa različitim nivoima pristupa (npr. korisnici, administratori, superadministratori).
- Svaka grupa ima ograničena prava u sistemu na osnovu **RBAC** modela.

---

4. Monitoring i detekcija pretnji

Praćenje događaja (logovanje)

- Sve aktivnosti korisnika (prijave, izmene podataka, greške) se beleže u sigurnosnim log fajlovima.
- Logovi se čuvaju u centralizovanom sistemu za nadzor (npr. **SIEM** – Security Information and Event Management).

Korišćenje AI za detekciju anomalija

- Implementiran je sistem koji pomoću **mašinskog učenja** analizira obrasce ponašanja korisnika, kao što su neobično vreme pristupa, nepoznate IP adrese, ili prekomerni broj neuspelih pokušaja prijave.
- U slučaju detekcije sumnjivog ponašanja, sistem automatski blokira nalog ili zahteva dodatnu verifikaciju.

5. Usklađenost sa pravnim regulativama

GDPR i zaštita privatnosti

- Korisnici su prilikom registracije informisani o načinu prikupljanja i korišćenja njihovih podataka, sa opcijom da daju ili povuku saglasnost.
- Sistem omogućava korisnicima da pregledaju, preuzmu ili izbrišu svoje podatke („pravo na zaborav“).
- U slučaju incidenta koji dovede do curenja podataka, kompanija ima obavezu da u roku od 72 sata obavesti nadležne organe i korisnike.

---

6. Plan za oporavak od incidenata

- Redovni backup podataka se pravi i čuva na sigurnim lokacijama.
- Postoji definisan plan reakcije na sigurnosne incidente, uključujući brzo otkrivanje, analizu, obaveštavanje i sanaciju.
- Tim za bezbednost je obučen za pravovremenu reakciju na napade i koordinaciju sa relevantnim službama.

---

7. Zaključak

Ovaj primer pokazuje kako se primenjuju različite bezbednosne tehnologije i prakse u realnoj poslovnoj aplikaciji, sa ciljem zaštite podataka korisnika i usklađivanja sa zakonodavnim zahtevima. Kroz enkripciju, višefaktorsku autentifikaciju, bezbednu komunikaciju, monitoring i primenu AI za detekciju pretnji, kompanija može da minimizira rizike i očuva poverenje svojih korisnika.