Datubāzes drošība

Pašpārbaudes tabula

Pašpārbaudes tabulā apkopotas drošības kontroles, kas ievērojamas datubāžu un tajās izvietoto datu drošībai. Tabula var kalpot par sākumpunktu pirmreizējā drošības pārbaudē vai izmantojama kā veidne izstrādājot pielāgotu audita plānu.

Rekomendējam veikt regulāras datubāzes drošības pārbaudes, lai pārliecinātos par datubāzes nocietināšanai veikto pasākumu pietiekamību.

*DB – datubāze

Fiziskā drošība

- [ ] Serveris/-i izvietoti drošā, slēgtā telpā ar serveru telpai atbilstošiem vides parametriem.
- [ ] Serveris/-i izvietoti telpā ar piekļuves kontroles sistēmu.
- [ ] Datubāze ir hostēta uz izolēta servera (vēlams arī fiziski nodalīta no WEB un aplikāciju servera).

Ugunsmūris

- [ ] DB serveris izvietots aiz ugunsmūra, kas pēc noklusējuma aizliedz visu ienākošo satiksmi.
- [ ] Datubāzes servera ugunsmūris atļauj tikai specifiskas aplikāciju vai WEB servisus, liegta tieša klienta piekļuve.
- [ ] Ja izstrādes vide nevar nodrošināt augstākminētos ugunsmūra parametrus, izstrādes videi izmanto testa datus. Produkcijas datu maskēšana nav uzskatāma par pietiekamu drošības kontroli.
- [ ] Ieviests izmaiņu kontroles process ugunsmūra kārtulām, sistēmu un DB administratori saņem paziņojumus par izmaiņām.
- [ ] DB un sistēmu administratori uztur un regulāri pārskata DB servera ugunsmūra kārtulas. Ārpakalpojuma izmantotos pakalpojumus regulāru pārskata drošības pārvaldnieks.
- [ ] Servera un aplikācijas līmeņa drošības kontroles un ugunsmūra uzstādījumi tiek regulāri testēti ar tīkla skaniem un drošības pārbaudēm.

Programmatūra

- [ ] Tiek izmantota ražotāja atbalstīta vai atvērtā pirmkoda (open source) DB programmatūras versija.
- [ ] Neizmantotie un nevajadzīgie DB servisi un funkcionalitāte ir izslēgta vai dzēsta.
- [ ] Ražotāja noklusētie konti ir dzēsti, bet, ja tehniskās iespējas to nepieļauj, tad kontiem ir uzstādītas drošas, vismaz 16 rakstzīmes garas paroles.
- [ ] Netiek izmantotas NULL paroles jeb konti bez parolēm.
- [ ] DB programmatūrai ir uzstādīti visi pieejamie drošības ielāpi. Ir ieviests process, lai savlaicīgi uzstādītu jaunākos drošības ielāpus un uzturētu programmatūras drošības līmeni.

Aplikāciju/WEB serveris

- [ ] Programmatūras kods ir pārbaudīts pret SQL injekciju ievainojamībām.
- [ ] Liegta pieeja konfigurācijas failiem un pirmkodam (source-code). Piekļuve ļauta tikai noteiktiem lietotāja kontiem.
- [ ] Visi serveri, programmatūra un rīki, kam ļauta piekļuve DB, ir uzskaitīti (dokumentēti).
- [ ] Ieviesti aizsardzības pasākumi gala sistēmām (programmām, WEB serveriem), kas izmantot DB datus, atbilstoši datu drošības prasībām. Visi serveri un klienti atbilst minimālajām drošības prasībām.

Darbstacijas

- [ ] Fizisko personu dati, kas ir nevajadzīgi, tiek periodiski dzēsti.
- [ ] Fizisko personu dati netiek pārsūtīti e-pastā (tekstā vai pielikuma formā). Pārsūtīšanu neveic gan lietotāji, gan sistēma automatizētu procesu ietvaros.
- [ ] Fizisko personu dati netiek uzglabāti uz pārvietojamām iekārtām.
- [ ] Ja lietotājiem ir ļauts izvietot fizisko personu datus uz darbstacijas, tad dati tiek šifrēti operētājsistēmas līmenī.
- [ ] Ja lietotājiem ir ļauts izvietot fizisko personu datus uz darbstacijas, tad darbstacijai ir individuāli lietotāja konti ar paroli.
- [ ] Ja lietotājiem ir ļauts izvietot fizisko personu datus uz darbstacijas, tad darbstacija ir aizsargāta pret neautorizētu piekļuvi ar ekrāna bloķēšanu. Lietotāji pārzina savu pienākumu veikt darbstacijas bloķēšanu atstājot darba vietu.
- [ ] Ja lietotājiem ir ļauts izvietot fizisko personu datus uz darbstacijas, tad darbstacijas atbilst minimālajām drošības prasībām.

Piekļuves kontrole

- [ ] DB administratori pārzina savus pienākumus, tai skaitā, atbildību pārskatīt izmaiņas DB un skriptos, lai nodrošinātu, ka sistēmas drošība netiek kompromitētā.
- [ ] Konti ar sistēmas administrēšanas tiesībām ir piešķirti pēc iespējas mazāk lietotājiem, bet ne mazāk kā divām personām.
- [ ] Operētājsistēmas konti, ko izmanto DB administratori piekļuvei DB, ir individuālai lietošanai paredzēti konti. Netiek izmantoti koplietošanas konti.
- [ ] Sistēmkontam, kas nepieciešams DB servera procesa palaišanai, nav ļauts veikt tiešu (direct) pieteikšanos. Tā vietā, tiek izmantoti operētājsistēmu konti un pēc nepieciešamības eskalētas privilēģijas - su vai sudo (UNIX) vai uz kontu, kam liegta standarta pieteikšanās darbstacijā (Windows).
- [ ] Operētājsistēmas konti, ko izmanto administrēšanai, ir individuālai lietošanai paredzēti konti. Netiek izmantoti koplietošanas konti.
- [ ] Koplietošanas konti ir pieļaujami DB automatizētiem apkopes vai monitoringa procesiem, piemēram, rezerves kopiju u.c.
- [ ] Koplietošanas konti netiek izmantoti ikdienas darbā. Konti var tikt izmantoti problēmu izmeklēšanai, apkopē un monitoringa darbos.
- [ ] Ar izstrādātājiem, izplatītājiem, sistēmu, DB administratoriem un kontraktoriem ir parakstīti neizpaušanas līgumi (NDA).
- [ ] DB operētājsistēmas un DB kontu paroles atbilst drošības prasībām. Paroles tiek periodiski mainītas, kad administrators/ kontraktors pārtrauc darba tiesiskās attiecības vai maina amata.
- [ ] Ja izstrādātāja un DB administratora lomu pilda viena persona, visas izmaiņas pārskata par drošību atbildīgā persona.

Lietotāju lomas un uzstādījumi

- [ ] Datubāzei izmanto drošu autentificēšanās mehānismu.
- [ ] Piekļuve datubāzei ir tikai autorizētiem lietotājiem.
- [ ] Piekļuves piešķiršanas un pārvaldības process ir dokumentēts. Datu īpašnieks ir apstiprinājis dokumentu ar parakstu.
- [ ] Lietotājiem tiek piešķirtas minimālās nepieciešamās tiesības amata ietvaros veicamo darbu izpildei. Atļaujas tiek pārvaldītas izmantojot lomas vai grupas, nevis tieši piešķirot lietotāja ID (ja tehniski iespējams).
- [ ] Ieviesta droša paroļu politika, ko atbalsta tehniski kontroles mehānismi. DB glabātās paroles un tīklā pārraidītās paroles tiek šifrētas.
- [ ] (Ja iespējams) Programmatūrām ir nepieciešama individuāla datubāzes pieteikšanās/parole un lomas/dotācijas. Ja to nav iespējams realizēt, var izmantot programmatūru kontus. Tomēr pieteikšanās ID un parole šajā gadījumā ir jāaizsargā, un šī informācija nevar būt pieejama uz darbstacijas.
- [ ] Programmatūrām tiek veikta lietotāju tiesību pārvaldība un auditēšana atbilstoši datu īpašnieka prasībām.
- [ ] DB objektiem, kas satur fizisko personu datus, nav publiskas atļautas (public grants). Visas piešķirtās publiskās atļaujas datubāzes objektiem, kas satur fizisko personu datus, ir dokumentētas.
- [ ] Visās vidēs (izstrādes, produkcijas u.c.), kur izvietoti fizisko personu dati, kontiem (ja vien tie nav DB administratori) nav ļauta lomu un atļauju piešķiršana (granting).
- [ ] DB konti tiek bloķēti pēc 5 nesekmīgu pieteikšanās mēģinājumu skaita.
- [ ] Neaktīvi lietotāja konti tiek periodiski identificēti. Process ir dokumentēts.
- [ ] Reizi ceturksnī tiek apkopota informācija par DB kontiem, kam piešķirtas priviliģētas tiesības.
- [ ] Tiek veikti lietotāju kontu un tiem piešķirto tiesību auditi. Auditi tiek veikti regulāri (rekomendējamais intervāls ir reizi pusgadā).

Datu drošība

- [ ] Datubāzē tiek glabāti tikai tādi fizisko personu dati, kas nepieciešami biznesa funkciju izpildei. Vēsturiskie dati tiek dzēsti, kad tie vairs nav nepieciešami.
- [ ] Netiek veikta datu dublēšana sistēmas ietvaros, un, kur vien iespējams, tiek novērsta datu ēnošana ārpus sistēmas. Ja dati ir nepieciešami tikai atbilstības pārbaudei, jāizmanto jaukšanas (hashing) funkcijas pirms datu saglabāšanas. Ja iespējams, nošķir fizisko personu datus no citiem datiem un glabā bezsaistē, līdz tie ir nepieciešami. Ja nepieciešams veikt fizisko personu datu pārsūtīšanu citām programmatūrām, uzturētājs ir informēts par datu drošības prasībām.
- [ ] Testa un izstrādes vidēm ir piemērotas tādas pašas drošības prasības kā produkcijas videi. Ja testa/izstrādes vides neatbilst drošības prasībām, dati šajās vidēs ir jāšifrē ar industrijas standarta algoritmiem, vai arī šīm sistēmām ir jāveido testa dati. Datu maskēšana nav uzskatāma par pietiekamu drošības kontroli.
- [ ] Fizisko personu datu atrašanās DB ir dokumentēta.
- [ ] Fizisko personu dati netiek izmantoti kā tabulu atslēgas.

Izmaiņu vadība

- [ ] Izmaiņu vadības process ir dokumentēts un atbilst biznesa prasībām.
- [ ] Visas izmaiņas produkcijas datubāzei tiek žurnalētas.
- [ ] Programmas, tai skaitā, WEB servisi, kas vai ko izmanto datubāze, ir dokumentēti un iekļauti audita tvērumā.

Auditēšana

- [ ] Auditācijas pierakstos (logs) tiek žurnalēti visi piekļuves mēģinājumi, sekmīgi un nesekmīgi.
- [ ] Sistēmas, aplikācijas un datubāzes līmeņa auditācijas pieraksti tiek uzglabāti atbilstoši biznesa un Ministru kabineta prasības (vismaz 6 vai 18 mēneši, atkarībā no sistēmas klases).
- [ ] Visām datubāzes komponentēm/ objektiem, kur tehniski iespējams, ir iespējota auditēšana.
- [ ] Auditācijas pieraksti tiek regulāri analizēti. Analīzi veic kompetenta persona, process ir dokumentēts.
- [ ] Par drošību atbildīgā persona saņem paziņojumus par bloķētiem lietotāja kontiem, kas veikuši maksimāli pieļaujamo nesekmīgu pieteikšanās mēģinājumu skaitu.
- [ ] Ieviests reāllaika notikumu monitorings, informējot DB administratoru par neautorizētām darbībām un piekļuves mēģinājumiem.

Rezerves kopijas

- [ ] Rezerves kopiju izveides un atjaunošanas process ir dokumentēts.
- [ ] Rezerves kopiju izveides un atjaunošanas process tiek regulāri testēts.
- [ ] Rezerves kopiju izveides grafiks atbilst RTO (Recovery Time Objective), RPO (Recovery Point Objective), biznesa nepārtrauktības un sistēmas pieejamības prasībām.
- [ ] Datu, t.sk. rezerves kopiju, uzglabāšanas ilgums atbilst normatīvo aktu prasībām.
- [ ] Rezerves kopiju failiem ir piemērotas līdzvērtīgas drošības kontroles kā produkcijas datiem.

Kriptogrāfija

- [ ] Tīkla komunikācija (datu pārraide, autorizēšanās process u.c.) norit pa šifrētiem kanāliem.
- [ ] Izmantotie kriptogrāfiskie mehānismi nodrošina datu aizsardzību, ja komunikācijas kanāls tiek pārtverts vai pārvirzīts.
- [ ] Ieviesti kriptogrāfiski mehānismi visos datu pārraides un apstrādes līmeņos (tīkla, aplikācijas, datubāzes).
- [ ] Kriptogrāfisko atslēgu pārvaldības process ir dokumentēts un atslēgas ir pieejamas vairāk kā vienai personai.
- [ ] Drošības pārvaldnieks jeb par IT drošību atbildīgā persona nosaka izmantošanai atļautos/ aizliegtos kriptogrāfiskos mehānismus.
- [ ] Lentās uzglabātie dati tiek šifrēti. Atslēgas netiek uzglabātas nešifrēti uz lentām.