BERILGANLAR BAZASIDA XAVFSIZLIK

Tojimamatov Isroil
Farg‘ona davlat universiteti amaliy matematika va informatika kafedrasi katta o’qituvchisi
israiltojimamatov@gmail.com
Soyipova Ominaxon Mirodiljon qizi
Farg‘ona davlat universiteti talabasi
soyipovaominaxon@gmail.com

Annotatsiya: Ushbu maqola berilganlar bazasida xavfsizlikning muhim jihatlarini ko'rib chiqadi. Maqolada berilganlarga ruxsatsiz kirish, ma'lumotlar buzilishi va yo'qolishining oldini olish uchun qo'llaniladigan asosiy xavfsizlik choralari, xavf-xatarlar va ularni bartaraf etish yo'llari tahlil qilinadi.

Kalit so'zlar: Berilganlar bazasi, xavfsizlik, ma'lumotlar himoyasi, ruxsatsiz kirish, ma'lumotlar buzilishi, xavf-xatarlar, zamonaviy texnologiyalar.

Annotation: This article examines the crucial aspects of security in databases. It analyzes key security measures, risks, and mitigation strategies employed to prevent unauthorized access, data corruption, and loss.

Keywords: Database, security, data protection, unauthorized access, data corruption, risks, modern technologies.

Аннотация: В данной статье рассматриваются важные аспекты безопасности в базах данных. Анализируются ключевые меры безопасности, риски и стратегии смягчения последствий, применяемые для предотвращения несанкционированного доступа, повреждения и потери данных.

Ключевые слова: База данных, безопасность, защита данных, несанкционированный доступ, повреждение данных, риски, современные технологии.

Kirish: Zamonaviy dunyoda ma'lumotlar muhim ahamiyat kasb etadi. Biznes, hukumat, ilm-fan, ta'lim va ko'plab boshqa sohalarda ma'lumotlarni saqlash, boshqarish va qayta ishlash uchun berilganlar bazalaridan keng foydalaniladi. Berilganlar bazalari, faktlar, raqamlar, matnlar va boshqa turdagi ma'lumotlarni tuzilgan holda saqlashga imkon beruvchi tizimlar bo'lib, ularning mavjudligi va samarali ishlashi bugungi raqamli iqtisodiyotning asosi hisoblanadi. Mijozlar ma'lumotlari, moliyaviy hisobotlar, ilmiy tadqiqot natijalari va shaxsiy ma'lumotlar kabi muhim ma'lumotlar berilganlar bazalarida saqlanadi.Shunday ekan, ma'lumotlar xavfsizligini ta'minlash dolzarb va muhim vazifadir. Berilganlar bazalariga ruxsatsiz kirish, ma'lumotlarning buzilishi yoki yo'qolishi jiddiy oqibatlarga olib kelishi

mumkin, jumladan, moliyaviy yo'qotishlar, reputatsiya buzilishi, qonuniy javobgarlik va shaxsiy ma'lumotlarning oshkor bo'lishi. Kiberhujumlar tobora murakkablashib borar ekan, berilganlar bazalarini himoya qilish uchun yangi usullar va texnologiyalarni doimiy ravishda ishlab chiqish va joriy etish zarur.Ushbu maqolaning maqsadi berilganlar bazasida xavfsizlikning asosiy jihatlarini o'rganish, mavjud tahdidlarni tahlil qilish va xavfsizlikni ta'minlash uchun samarali choralarni ko'rsatishdan iborat. Maqolada, shuningdek, berilganlar bazasi xavfsizligini ta'minlashda zamonaviy texnologiyalar va usullarning roli ham o'rganiladi. Maqola qamrovi quyidagi mavzularni o'z ichiga oladi: berilganlar bazasiga tahdidlar, autentifikatsiya va avtorizatsiya, ma'lumotlarni shifrlash, auditorlik, SQL injeksiyasidan himoya, zaxira nusxalarini yaratish va tiklash, xavfsizlik siyosati va standartlari, ma'lumotlar niqoblash, sun'iy intellekt va blokcheyn texnologiyasi.

Berilganlar bazalari turli xil tahdidlar va xavf-xatarlarga duch kelishi mumkin. Bu tahdidlar berilganlar bazasining maxfiyligini, yaxlitligini va mavjudligini buzishi mumkin. Tahdidlarni aniqlash va tushunish xavfsizlik choralarini samarali rejalashtirish va amalga oshirish uchun muhimdir. Tahdidlarni kelib chiqish manbaiga ko'ra ichki va tashqi tahdidlarga bo'lish mumkin. Ichki tahdidlar tashkilot ichidagi shaxslar (xodimlar, pudratchilar yoki boshqa vakolatli foydalanuvchilar) tomonidan kelib chiqadi. Ushbu turdagi tahdidlar tashkilotning o'zida xavfsizlik siyosati va protseduralariga rioya qilmaslik natijasida yuzaga kelishi mumkin.

Ruxsatsiz foydalanuvchilarning kirishi: Berilganlar bazasiga kirish huquqi bo'lmagan shaxslarning ma'lumotlarga kirishga urinishi. Bu zaif parollar, noto'g'ri konfiguratsiya qilingan ruxsatlar yoki xodimlarning hisob ma'lumotlarini o'g'irlash orqali sodir bo'lishi mumkin. Ichki xodimlar tomonidan suiiste'mol qilish: Berilganlar bazasiga kirish huquqiga ega bo'lgan xodimlarning o'z vakolatlarini suiiste'mol qilishi. Bu ma'lumotlarni o'g'irlash, o'zgartirish yoki yo'q qilish, shuningdek, shaxsiy maqsadlarda ma'lumotlardan foydalanishni o'z ichiga olishi mumkin. Misol uchun, xodimlar mijozlar ro'yxatini sotishlari yoki raqobatchilarga oshkor qilishlari mumkin. Noto'g'ri konfiguratsiya va boshqaruv: Berilganlar bazasini noto'g'ri konfiguratsiya qilish yoki xavfsizlikni noto'g'ri boshqarish xavfsizlik zaifliklarini keltirib chiqarishi mumkin. Misol uchun, sukut bo'yicha parollardan foydalanish, yangilanishlarni o'rnatmaslik yoki noto'g'ri ruxsatlarni sozlash tahdidlarga yo'l ochishi mumkin.

Tashqi tahdidlar tashkilot tashqarisidagi shaxslar yoki tashkilotlar tomonidan kelib chiqadi. Ushbu turdagi tahdidlar odatda kiberhujumlar orqali amalga oshiriladi va berilganlar bazasiga ruxsatsiz kirish, ma'lumotlarni o'g'irlash yoki zarar yetkazishni maqsad qiladi. SQL injeksiyasi: Xakerlar zaif veb-ilovalar orqali berilganlar bazasiga zararli SQL kodini kiritishga urinishadi. Bu ruxsatsiz kirish, ma'lumotlarni o'g'irlash yoki o'zgartirishga olib kelishi mumkin. DDoS hujumlari (Distributed Denial of Service): Xakerlar berilganlar bazasiga juda ko'p so'rovlar yuborib, uning ishdan

chiqishiga yoki foydalanuvchilar uchun mavjud bo'lmay qolishiga sabab bo'lishadi. Viruslar va zararli dasturlar: Viruslar, troyanlar, qurtlar va boshqa zararli dasturlar berilganlar bazasiga zarar yetkazishi, ma'lumotlarni o'g'irlashi yoki tizimning ishdan chiqishiga olib kelishi mumkin. Tarmoq xavfsizligi muammolari: Zaif tarmoq xavfsizligi, noto'g'ri konfiguratsiya qilingan himoya devorlari yoki zaif simsiz tarmoqlar xakerlarga berilganlar bazasiga kirishga imkon berishi mumkin.

Zamonaviy axborot texnologiyalari davrida ma'lumotlar bazasi (MB) kompaniya va tashkilotlarning eng qimmatli resurslaridan biri hisoblanadi. Shu sababli, MB xavfsizligini ta'minlash juda muhim vazifa bo'lib, uning buzilishi katta moliyaviy va obro'-e'tibor zararlariga olib kelishi mumkin. Quyida berilganlar bazasini himoya qilish uchun asosiy chora-tadbirlar ko'rib chiqiladi. Autentifikatsiya va avtorizatsiya ma'lumotlar bazasi foydalanuvchilarini aniqlash va ularga tegishli ruxsatlarni taqsimlash xavfsizlikning poydevori hisoblanadi. Kuchli parollar siyosati: Foydalanuvchilar murakkab va oson topilmaydigan parollardan foydalanishi, parollar muntazam yangilanib turishi kerak. Ko'p faktorli autentifikatsiya (MFA): Foydalanuvchini faqat parol orqali emas, balki qo'shimcha tasdiqlash (masalan, SMS orqali kod, biometrik ma'lumotlar) orqali aniqlash xavfsizlik darajasini oshiradi. Rolga asoslangan ruxsatlarni boshqarish (RBAC): Har bir foydalanuvchiga faqat uning ish faoliyati uchun zarur bo'lgan minimal huquqlar beriladi. Kam imtiyozlar prinsipi: Har bir foydalanuvchi yoki dastur faqat o'z vazifasini bajarish uchun zarur bo‘lgan eng kam darajadagi huquqlarga ega bo‘lishi kerak.

Ma'lumotlar bazasidagi ma'lumotlarning maxfiyligini ta'minlash uchun ularni shifrlash muhim hisoblanadi. Ma'lumotlarni harakatda shifrlash (SSL/TLS): Tarmoq orqali uzatilayotgan ma'lumotlar shifrlanib, ularni ushlash yoki o‘zgartirish xavfi kamayadi. Ma'lumotlarni saqlashda shifrlash (TDE): Berilganlar bazasida saqlanayotgan ma'lumotlar shifrlanadi, bu esa ruxsatsiz kirish holatlarida ma'lumotlarning o‘qilmasligini ta'minlaydi. Shifrlash kalitlarini boshqarish: Kalitlar xavfsiz joyda saqlanib, ularning ruxsatsiz foydalanilishi oldi olinadi. Auditorlik – ma'lumotlar bazasidagi harakatlarni qayd etish va tahlil qilish xavfsizlikni ta'minlashning muhim qismidir. Foydalanuvchi harakatlarini kuzatish va yozib borish: Kim, qachon va qanday amallarni bajarganini yozib borish orqali muammolar paydo bo‘lganda ularni aniqlash osonlashadi. Xavfsizlik hodisalarini aniqlash va javob berish: Anomaliyalar yoki hujumlar darhol aniqlanib, ularga tezkor javob beriladi. Doimiy monitoring va tahlil: MB faoliyati doimiy ravishda nazorat qilib boriladi, shubhali holatlar aniqlanadi.

Ma'lumotlar niqoblash (Data Masking) - nu usulda maxfiy ma'lumotlar maxsus texnikalar yordamida yashiriladi yoki o‘zgartiriladi, shunda ularni ko‘rgan odam asl ma'lumotni bilolmaydi. Asosan testlash va ishlab chiqish muhitlarida ishlatiladi, chunki haqiqiy ma'lumotlarni to‘liq ochish xavfsizlikka zarar yetkazishi mumkin.

Masalan, bank kartalari, shaxsiy identifikatsiya raqamlari yoki boshqa maxfiy ma'lumotlar niqoblanadi, lekin ularning ko‘rinishi test uchun yetarli bo‘ladi. Ma'lumotlar klassifikatsiyasi - bu jarayon ma'lumotlarni ularning sezgirlik darajasiga ko‘ra guruhlashni bildiradi. Masalan, ma'lumotlar: umumiy, ichki, maxfiy, yoki juda maxfiy kabi kategoriyalarga bo‘linadi. Har bir turdagi ma'lumot uchun alohida xavfsizlik choralari qo‘llanadi, masalan, juda maxfiy ma'lumotlar uchun kuchli shifrlash va qattiq kirish nazorati. Bu klassifikatsiya kompaniyaning xavfsizlik siyosatini aniq va samarali qilishga yordam beradi. Sun'iy intellekt va mashinaviy o'rganish - bu texnologiyalar xavfsizlik sohasida juda ko‘p qo‘llaniladi. Hujumlarni aniqlash va oldini olish uchun AI tizimlari tarmoq trafigini tahlil qilib, g‘ayrioddiy faollikni aniqlaydi. Anormalliklarni aniqlashda mashinaviy o‘rganish algoritmlari kundalik faoliyatdan chetga chiqqan holatlarni topadi. Xavfsizlikni avtomatlashtirish esa inson omilini kamaytirib, tezkor va aniq choralar ko‘rishga imkon beradi. Blokcheyn texnologiyasi - Blokcheyn ma'lumotlar yaxlitligini ta'minlaydi, ya'ni ma'lumotlar o‘zgartirilmaganligini kafolatlaydi. Har bir ma'lumot bloki oldingi blok bilan bog‘langan va o‘zgartirish uchun barcha bloklarni qayta yozish kerak bo‘ladi, bu esa firibgarlikni qiyinlashtiradi. Auditorlik izlari yaratish orqali har qanday o‘zgarishlar aniq qayd etiladi, bu esa mas’uliyatni oshiradi va tekshiruvlarni osonlashtiradi.

Katta ma'lumotlar bazalarining o'ziga xos xususiyatlari va xavfsizlik muammolari - katta ma'lumotlar (Big Data) odatda hajmi juda katta, tezligi yuqori va turli xil formatlarda bo‘ladi (strukturali, nostrukturali, yarim strukturali). Ushbu xususiyatlar xavfsizlikni ta'minlashni murakkablashtiradi, chunki ma'lumotlarni saqlash, uzatish va qayta ishlash jarayonlari ko‘p miqdorda va tez sodir bo‘ladi. Katta ma'lumotlar bazalarida quyidagi xavfsizlik muammolari yuzaga keladi: Ma'lumotlarning maxfiyligi va yaxlitligini ta'minlash qiyinligi. Kirish nazoratining murakkabligi, chunki ko‘p foydalanuvchilar va tizimlar ishlaydi. Ma'lumotlar oqimining katta bo‘lishi tufayli hujumlarni aniqlash va oldini olish qiyinlashadi. Zaxira qilish va tiklash jarayonlarida xavfsizlikni ta'minlash. Hadoop va Spark kabi katta ma'lumotlarni qayta ishlash platformalari keng qo‘llaniladi, lekin ularni himoya qilish uchun maxsus choralar talab etiladi. Hadoopda Kerberos autentifikatsiyasi yordamida foydalanuvchilarni aniqlash va kirishni boshqarish amalga oshiriladi. Shuningdek, ma'lumotlarni shifrlash (diskda va tarmoqlarda) xavfsizlikni oshiradi. Sparkda ham xavfsizlik qatlamlari mavjud, masalan, autentifikatsiya, avtorizatsiya va shifrlash. Rollarga asoslangan kirish nazorati (RBAC) va audit loglar yordamida tizimdagi harakatlar nazorat qilinadi. Tarmoqqa kirish uchun xavfsiz protokollar (masalan, TLS) qo‘llaniladi.

Xulosa:

Maqolada berilganlar bazasining xavfsizligi bilan bog‘liq muhim jihatlar keng qamrovda ko‘rib chiqildi. Zamonaviy dunyoda ma'lumotlar bazalari biznes va jamiyat

hayotida katta ahamiyatga ega bo‘lib, ularning himoyasi har doim ustuvor vazifa hisoblanadi. Ichki va tashqi tahdidlar, shuningdek, inson omili xavfsizlikning asosiy zaifliklari bo‘lib, ularga qarshi samarali chora-tadbirlar joriy etilishi zarur. Maqolada autentifikatsiya, avtorizatsiya, ma'lumotlarni shifrlash, auditorlik va SQL injeksiyalaridan himoya kabi an'anaviy xavfsizlik usullari bilan bir qatorda, zamonaviy texnologiyalar – ma'lumotlar niqoblash, sun'iy intellekt, blokcheyn va katta ma'lumotlar bazalarining o‘ziga xos xavfsizlik muammolari ham batafsil tahlil qilindi. Bulutli berilganlar bazalarida xavfsizlikni ta'minlash masalalari ham alohida e'tibor qaratildi. Kelajakda sun'iy intellekt va avtomatlashtirish texnologiyalarining roli yanada oshishi, yangi tahdidlar paydo bo‘lishi ehtimoli mavjud. Shu sababli, berilganlar bazasi xavfsizligini ta'minlashda doimiy monitoring, yangilanishlar va takomillashtirish muhim ahamiyat kasb etadi. Xulosa qilib aytganda, ma'lumotlar bazalarini himoya qilish uchun ko‘p qirrali yondashuv va zamonaviy texnologiyalardan samarali foydalanish zarur bo‘lib, bu sohadagi xavfsizlik siyosati va amaliyotlar doimiy ravishda rivojlanib borishi lozim.

Foydalanilgan adabiyotlar:

1. Kent, S. T., & Frankel, Y. (2012). NIST Special Publication 800-63-3: Digital Identity Guidelines. National Institute of Standards and Technology (NIST).
2. Ferraiolo, D. F., Sandhu, R. S., Gavrila, S., Kuhn, D. R., & Chandramouli, R. (2001). Role-Based Access Control. Artech House.
3. Schneier, B. (1996). Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons.
4. Oracle Documentation / Microsoft SQL Server Documentation / PostgreSQL Documentation. (Tegishli ma'lumotlar bazasi tizimlarining rasmiy hujjatlari).
5. ISO/IEC 27002. Information technology — Security techniques — Code of practice for information security controls.
6. CIS (Center for Internet Security) Benchmarks. (Ma'lumotlar bazalari uchun xavfsizlik konfiguratsiyasi bo'yicha amaliy qo'llanmalar).
7. OWASP (Open Web Application Security Project) Top 10. (Web-ilovalar xavfsizligi bo'yicha dolzarb ma'lumotlar).
8. Data Masking Solutions Providers' Whitepapers. (Masalan, Informatica, IBM, Broadcom kabi kompaniyalarning texnik hisobotlari).
9. Research papers on "AI in Cybersecurity" or "Machine Learning for Anomaly Detection in Databases" (Masalan, IEEE Transactions on Dependable and Secure Computing, ACM Computing Surveys kabi nufuzli ilmiy jurnallardan).
10. Vacca, J. R. Computer Security Handbook. Auerbach Publications.