

MA'LUMOTLAR BAZASIDA XAVFSIZLIKNI TA'MINLASH

Umid Ortikov Alisher o'g'li

IT PARK Universiteti Dasturiy ta'minot muhandisligi fakulteti talabasi
+998915206101

umiddear@gmail.com

Shaxzod Ortikov Alisher o'g'li

IT PARK Universiteti Dasturiy ta'minot muhandisligi fakulteti talabasi
+998906014933

ortikoff@icloud.com

Kalit so'zlar: ma'lumotlar bazasi, kiberxavfsizlik, ma'lumotlar bazasini ta'minlash, kiber makon tushunchasi.

Annotatsiya

Axborot xavfsizligi tushunchasi kundan kunga glaballashib bormoqda, ayniqsa kundankunga axborot xurujlari va kiberjinoyatlar sonining ortib borishi xavfsizlik tushunchasining qanchalik global ekanligini ko'rsatmoqda. Axborot turli shakilda va turli saqlovchilarda saqlanishi mumkin bu axborotni saqlashning yangi texnologiyalarini ishlab chiqishni talab qiladi. Axborotni ma'lumotlar bazasida himoylash murakkab va texnologik jarayondir.

Ma'lumotlar bazasi xavfsizligi deganda ma'lumotlar bazasining maxfiyligi, yaxlitligi va mavjudligini o'rnatish va saqlash uchun mo'ljallangan vositalar, boshqaruv vositalari va chora-tadbirlar majmuasi tushuniladi. Axborotni ma'lumotlar bazasida xavfsizligi quyidagilarni hal qilishi va himoya qilishi quyidagilardan iborat:

- Ma'lumotlar bazasidagi ma'lumotlar;
- Ma'lumotlar bazasini boshqarish tizimi (DBMS);
- Har qanday bog'liq ilovalar;
- Jismoniy ma'lumotlar bazasi serveri va/yoki virtual ma'lumotlar bazasi serveri va asosiy uskuna;
- Ma'lumotlar bazasiga kirish uchun foydalaniladigan hisoblash va/yoki tarmoq infratuzilmasi.

Ma'lumotlar bazasi xavfsizligi axborot xavfsizligi texnologiyalari va amaliyotlarining barcha jihatlarini o'z ichiga olgan murakkab va qiyin ishdir. Bundan tashqari, bu ma'lumotlar bazasidan foydalanishga to'g'ri kelmaydi. Ma'lumotlar bazasi qanchalik qulay va foydalanish mumkin bo'lsa, u xavfsizlik tahdidlariga nisbatan zaifroq bo'ladi; ma'lumotlar bazasi tahdidlarga qanchalik daxlsiz bo'lsa, unga kirish va undan foydalanish shunchalik qiyin bo'ladi.

Ko'pgina dasturiy ta'minotning noto'g'ri konfiguratsiyasi, zaifliklar yoki ehtiyotsizlik yoki noto'g'ri foydalanish shakllari buzilishlarga olib kelishi mumkin. Quyida ma'lumotlar bazasi xavfsizligi hujumlarining eng keng tarqalgan turlari yoki sabablari va ularning sabablari keltirilgan:

- Ichki tahdidlar;
- Insayder tahdid - bu ma'lumotlar bazasiga imtiyozli kirish huquqiga ega bo'lgan uchta manbadan birining xavfsizlikka tahdididir;
- Zarar etkazmoqchi bo'lgan yomon niyatli insayder;

– Ma'lumotlar bazasini hujumga qarshi himoyasiz qiladigan xatolarga yo'l qo'yadigan beparvo insayder;

– Infiltrator - bu qandaydir tarzda fishing kabi sxema orqali yoki hisob ma'lumotlari ma'lumotlar bazasiga kirish orqali hisob ma'lumotlarini oladigan begona shaxs.

Ma'lumotlar bazasiga xos tahdid bo'lib, ular veb-ilovalar yoki HTTP sarlavhalari tomonidan xizmat ko'rsatadigan ma'lumotlar bazasi so'rovlariga o'zboshimchalik bilan SQL yoki SQL bo'lmagan hujum satrlarini kiritishni o'z ichiga oladi. Xavfsiz veb-ilovalarni kodlash amaliyotiga rioya qilmaydigan va muntazam zaiflik sinovlarini o'tkazadigan tashkilotlar ushbu hujumlarga ochiq¹.

Ma'lumotlar bazasi xavfsizligi axborot xavfsizligi texnologiyalari va amaliyotlarining barcha jihatlarini o'z ichiga olgan murakkab va qiyin ishdir. Bundan tashqari, bu ma'lumotlar bazasidan foydalanishga to'g'ri kelmaydi. Ma'lumotlar bazasi qanchalik qulay va foydalanish mumkin bo'lsa, u xavfsizlik tahdidlariga nisbatan zaifroq bo'ladi; ma'lumotlar bazasi tahdidlarga qanchalik daxlsiz bo'lsa, unga kirish va undan foydalanish shunchalik qiyin bo'ladi.

Rivojlanayotgan IT muhiti ma'lumotlar bazalarini tahdidlarga nisbatan sezgirroq qiladi. Ma'lumotlar bazalariga hujumlarning yangi turlariga olib kelishi mumkin bo'lgan yoki yangi mudofaa choralarini talab qilishi mumkin bo'lgan tendentsiyalar:

O'sib borayotgan ma'lumotlar hajmi - saqlash, ma'lumotlarni yig'ish va qayta ishlash deyarli barcha tashkilotlarda eksponent ravishda o'sib bormoqda. Har qanday ma'lumotlar xavfsizligi amaliyoti yoki vositalari uzoq va yaqin kelajakdagi talablarni qondirish uchun yuqori darajada kengaytirilishi kerak.

Tarqalgan infratuzilma - tarmoq muhitlari murakkablashib bormoqda, ayniqsa korxonalar ish yuklarini gibrud bulut yoki ko'p bulutli arxitekturaga o'tkazar ekan, bu xavfsizlik echimlarini joylashtirish, boshqarish va tanlashni qiyinlashtiradi.

Borgan sari qat'iy tartibga soluvchi talablar - butun dunyo bo'ylab tartibga solishga muvofiqlik landshafti murakkablashib bormoqda, shuning uchun barcha mandatlarga rioya qilish yanada qiyinlashmoqda.

Kiberxavfsizlik bo'yicha ko'nikmalar yetishmasligi - global kiberxavfsizlik bo'yicha malakali mutaxassislarining etishmasligi va tashkilotlar xavfsizlik rollarini to'ldirishda qiynalmoqda. Bu muhim infratuzilmani, jumladan ma'lumotlar bazalarini himoya qilishni qiyinlashtirishi mumkin.

FOYDALANILGAN ADABIYOTLAR RO'YXATI

1. O'zbekiston Respublikasi Prezidentining "Axborot texnologiyalari va kommunikatsiyalarining joriy etilishini nazorat qilish, ularni himoya qilish tizimini takomillashtirish chora-tadbirlari to'g'risida" qarori

2. O'zbekiston Respublikasi Axborotlashtirish va telekommunikatsiyalar sohasida nazorat bo'yicha davlat inspeksiyasi to'g'risidagi nizom

3. Kessler, Gari (2006 yil 17 noyabr). "Kriptografiyaga umumiy nuqtai". Prinston universiteti.

¹ Kessler, Gari (2006 yil 17 noyabr). "Kriptografiyaga umumiy nuqtai". Prinston universiteti.