MA’LUMOTLAR XAVFSIZLIGINI HIMOYA QILISH USULLARI VA TAHLILI

Ruzimov Omon Narimanovich
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti. Axborotlarni himoyalash usullari va tizimlari. Axborot xavfsizligi

Annotatsiya: *Ushbu maqolada Axborot xavfsizligida ma’lumotlarga qaratilgan hujumlarni himoya qilish usullari tahlil qilingan. Shuningdek, Ma’lumotni himoya qilish jismoniy shaxslar, korxonalar va barcha o‘lchamdagi tashkilotlar uchun muhim masaladir. Shu sababli ma’lumotlarni himoya qilish hozirgi kunda dolzarb masala bo‘lib hisoblanadi.*

Kalit so‘zlar: *Axborot xavfsizligi, kiberxavfsizlik, tarmoq xavfsizligi, jismoniy xavfsizlik, shifrlash, zaxiralash va tiklash, kirish nazorati, internet jihozlarni xavfsizligi. ma’lumotlarni himoyalash.*

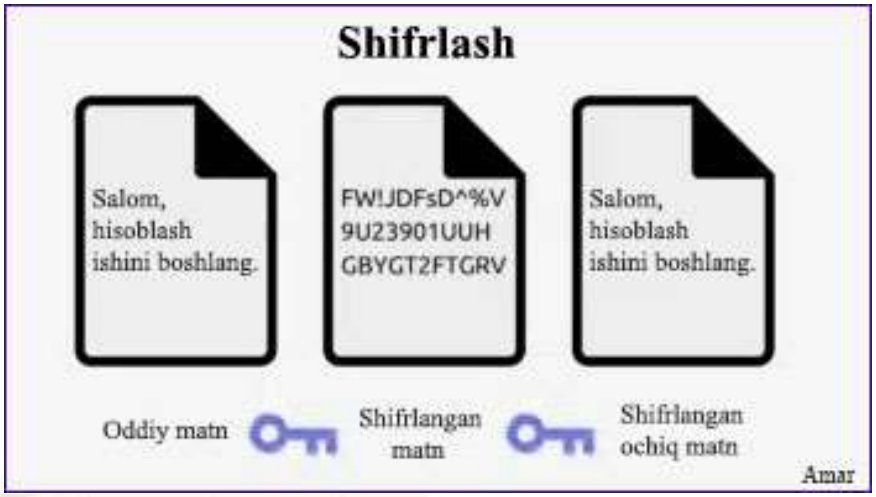
Kirish

Hozirgi kunda raqamli ma’lumotlarni himoyalash juda dolzarb masalalardan biri bo‘lib, ma’lumotlarni ishonchli saqlash va ulardan to‘g‘ri foydalanish juda zarur deb maqsad qilingan. Shuningdek, ma’lumotni himoya qilish jismoniy shaxslar, korxonalar va barcha o‘lchamdagi tashkilotlar uchun muhim masaladir. Muhim bo‘lgan ma’lumotlarni saqlash va ularni havfsiz uzatish texnologiyasiga bo‘lgan ishonch ortib borayotganligi sababli, ma’lumotlarning buzilishi va o‘g‘irlanishi tahdidi asosiy muammoga aylandi. 2023-yilda tahminan 4000 dan ortiq ochiq ma’lumotlar buzilishi sodir bo‘ldi, ularning 60% xakerlik natijasida sodir bo‘ldi. Ta’sir qilingan kompaniyalar va jismoniy shaxslar moliyaviy va obro‘-e’tiborini yo‘qotish, ma’lumotlarning buzilishi va ba’zan qonuniy javobgarlik xavfi ostida qolgan edi.

Ushbu xavflarni kamaytirish uchun ma’lumotlarni ruxsatsiz kirish va manipulyatsiyadan himoya qilishning bir qancha usullari ishlab chiqilgan. Ma’lumotlarni himoya qilishning eng asosiy usullarini batafsil yoritib berilgan.

Shifrlash

Shifrlash shaxsiy ma’lumotlarni himoya qilishning asosiy komponentidir. Bu shaxsiy ma’lumotlarni kodlangan shaklga aylantirishni o‘z ichiga oladi, bu esa tegishli shifrni ochish kaliti bo‘lmasa, uni hech kim o‘qib bilmaydi. Faqat shifrni ochish kalitiga ega bo‘lgan vakolatli foydalanuvchi ma’lumotni dekodlashi va ko‘rishi mumkin. Ushbu usul internet orqali uzatish paytida nozik ma’lumotlarni himoya qilish, shuningdek, noutbuklar va mobil telefonlar kabi qurilmalarda saqlangan ma’lumotlarni himoya qilish uchun keng qo‘llaniladi. Bundan tashqari, AES va RSA kabi shifrlash algoritmlari ma’lumotlarni shifrlash uchun ishlatiladi, bu esa ruxsatsiz foydalanuvchilarning ularga kirishini deyarli imkonsiz qiladi.



1-rasm. Shifrlash jarayoni

Shifrlashning asosiy afzalliklaridan biri shundaki, u ma’lumotlar buzilgan taqdirda ham yuqori darajadagi xavfsizlikni ta’minlaydi. Agar shifrlangan ma’lumotlar o‘g‘irlangan bo‘lsa yoki ruxsatsiz shaxs tomonidan boshqa yo‘l bilan foydalanilsa, ularni o‘qib bo‘lmaydi va shuning uchun tajovuzkor uchun foydasiz bo‘ladi. Bundan tashqari, shifrlash tashkilotlarga umumiy ma’lumotlarni himoya qilish to‘g‘risidagi nizom (GDPR) va to‘lov kartalari sanoati ma’lumotlar xavfsizligi standarti (PCI DSS) kabi maxfiylik qoidalari va standartlariga rioya qilishga yordam beradi.

Biroq, shifrlash ishonchli emas va samarali bo‘lishi uchun uni to‘g‘ri amalga oshirish kerak. Misol uchun, agar shifrlash kaliti yo‘qolsa yoki o‘g‘irlansa, shifrlangan ma’lumotlarga hatto qonuniy egasi ham kira olmaydi. Bundan tashqari, shifrlash algoritmlarini buzish mumkin, ayniqsa, agar ular texnologiya yutuqlari va zararli aktyorlarning hujumlari bilan tanishish uchun yangilanmasa.

Zaxiralash va tiklash

Ma’lumotlarni muntazam ravishda zaxiralash ma’lumotlarni himoya qilishning muhim jihati hisoblanadi, chunki u ma’lumotlar yo‘qolishi yoki buzilgan taqdirda ma’lumotlarning saqlanishini ta’minlaydi. Ma’lumotlar nusxalarini yaratish va ularni xavfsiz joyda saqlash orqali tashkilotlar falokat yuz berganda o‘z ma’lumotlarini tezda tiklashlari mumkin.

Zaxiralash va tiklashning asosiy afzalliklaridan biri shundaki, u tashkilotlarga ma’lumotlar yo‘qolishidan tezda tiklanish, ishlamay qolish vaqtini kamaytirish va ma’lumotlarning doimiy yo‘qolishi xavfini kamaytirish imkonini beradi. Bundan tashqari, zaxira va tiklash yechimlari qo‘shimcha xavfsizlik darajasini ham ta’minlashi mumkin, chunki ular ruxsat etilmagan o‘zgarishlar yoki o‘chirishlarni samarali ravishda bekor qilib, ma’lumotlarni oldingi vaqtga tiklash uchun ishlatilishi mumkin.

2-rasm. Ma’lumotlarni saqlash va ularni qayta ishlash serveri

Foydali bo‘lsa-da, ma’lumotlarni zaxiralash va tiklash faqat ular joylashtirilgan muhit kabi muvaffaqiyatli bo‘ladi. Zaxira nusxalari o‘g‘irlik, tabiiy ofat va boshqa xavflardan himoya qilish uchun xavfsiz joyda, masalan, saytdan tashqarida saqlanishi kerak. Bundan tashqari, falokat yuz berganda ularni muvaffaqiyatli tiklashga ishonch hosil qilish uchun zaxira nusxalari muntazam ravishda sinovdan o‘tkazilishi kerak.

Kirish nazorati

Kirish nazorati - bu maxfiy ma’lumotlarga kirishni faqat ruxsat berilgan foydalanuvchilar uchun cheklash usuli. Bunga parollardan foydalanish, ko‘p faktorli autentifikatsiya va rolga asoslangan kirishni boshqarish orqali erishish mumkin. Ushbu usullar faqat tegishli avtorizatsiyaga ega bo‘lganlar maxfiy ma’lumotlarga kirishini ta’minlaydi, ma’lumotlarning buzilishi va ruxsatsiz kirish xavfini kamaytiradi.

Kirish nazoratining asosiy afzalliklaridan biri shundaki, u tashkilotlarda kimning qanday resurslarga kirish huquqi borligini va kim qaysi harakatlarni amalga oshirganligini kuzatish va kuzatish imkonini berib, ichki tahdidlar xavfini kamaytirish orqali tashkilotlarda javobgarlikni o‘rnatishga yordam beradi. Bundan tashqari, kirishni boshqarish, kirish ruxsatlarini boshqarishni soddalashtirish orqali samaradorlikni oshiradi; ko‘p sonli foydalanuvchilar uchun kirishni boshqarish uchun zarur bo‘lgan vaqt va resurslarni qisqartirish.

3-rasm. Kirish nazorati

Ma’lumotlarni himoya qilishning barcha usullari singari, kirishni boshqarish samarali bo‘lishi uchun to‘g‘ri amalga oshirilishi kerak. Misol uchun, parollar kuchli va noyob bo‘lishi kerak va qo‘shimcha xavfsizlik darajasini ta’minlash uchun ko‘p faktorli autentifikatsiyadan foydalanish kerak. Bundan tashqari, kirishni boshqarish tizimlari to‘g‘ri ishlashi va maxfiy ma’lumotlarni ruxsatsiz kirishdan himoya qilish uchun muntazam ravishda yangilanishi va sinovdan o‘tkazilishi kerak.

Tarmoq xavfsizligi

Tarmoq xavfsizligi deganda kompyuter tarmoqlarida saqlanadigan ma’lumotlar va aktivlarni ruxsatsiz kirish, o‘g‘irlik yoki shikastlanishdan himoya qilish uchun qo‘llaniladigan chora-tadbirlar tushuniladi. Bunga ruxsatsiz kirishni blokirovka qilish uchun xavfsizlik devorlaridan foydalanish, kiberhujumlarni kuzatish va oldini olish uchun tajovuzni aniqlash tizimlarini joriy etish va tarmoq orqali uzatiladigan maxfiy ma’lumotlarni himoya qilish uchun shifrlashdan foydalanish kiradi. Dasturiy ta’minotni muntazam yangilash va xodimlarni o‘qitish ham kiberhujumlar xavfini kamaytirishda muhim rol o‘ynashi mumkin.

Tarmoq xavfsizligining asosiy afzalliklaridan biri uning maxfiylikdagi rolidir. Tarmoq xavfsizligi maxfiy ma’lumotlarning maxfiyligini ta’minlashga yordam beradi, ruxsatsiz kirish va ma’lumotlar buzilishining oldini oladi. Shuningdek, u tashkilotlarga HIPAA va PCI DSS kabi tartibga soluvchi talablar va sanoat muvofiqlik standartlariga javob berishga imkon beradi. Eng muhimi, tarmoq xavfsizligi xavflarni boshqarishda katta rol o‘ynaydi. Bu tashkilotlarga potentsial xavfsizlik xavflarini aniqlash va kamaytirishga yordam beradi, xavfsizlikni buzish va boshqa hodisalar ehtimolini kamaytiradi.

4-rasm. Tarmoqlar

Muvaffaqiyatli tarmoq xavfsizligi infratuzilmasi bilimli IT jamoasini talab qilishini ta’kidlash muhimdir. Tarmoq xavfsizligi tizimlari murakkab va boshqarish qiyin bo‘lishi mumkin, ularni samarali sozlash va saqlash uchun maxsus bilim va tajribani talab qiladi. Bundan tashqari, tahdidlar rivojlanib borar ekan, rivojlanayotgan tahdidlar va yangi hujum usullari bilan hamnafas bo‘lish uchun tarmoq xavfsizligi choralari doimiy ravishda yangilanishi va takomillashtirilishi kerak.

Jismoniy xavfsizlik

Jismoniy xavfsizlik ma’lumotlarni himoya qilishning yana bir muhim tarkibiy qismidir, chunki u nozik ma’lumotlarni saqlaydigan jismoniy qurilmalar va ob’ektlarni himoya qilish uchun qo‘llaniladigan choralarni o‘z ichiga oladi. Bu xavfsiz saqlash kabinetlari yoki omborlarida qulflash moslamalarini, biometrik autentifikatsiya yoki kalit kartalar bilan kirishni boshqarish tizimlarini joriy qilishni va nozik joylarda xavfsizlik kameralari va signallarni o‘rnatishni o‘z ichiga olishi mumkin. Noutbuklar va mobil telefonlar kabi portativ qurilmalar ham o‘g‘irlanishi yoki yo‘qolishi mumkin va ularni shifrlash, xavfsiz parollar va masofadan o‘chirish imkoniyatlari bilan himoyalanishi mumkin.

5-rasm. Jismoniy xavfsizlik

Jismoniy xavfsizlikning aniq ijobiy tomoni - bu tashkilotlarga ishonch. Jismoniy xavfsizlik choralari tashkilotlarga o‘zlarining zahiraviy ma’lumotlarining yaxlitligi va mavjudligiga ishonch hosil qilishi, ma’lumotlarning yo‘qolishi yoki buzilishi xavfini kamaytirishi mumkin. Tashkilotlar, shuningdek, zaxira vositalarini himoya qilish orqali xarajatlarni kamaytirishi mumkin, chunki ular lenta yoki qattiq disklardan ma’lumotlarni tiklash kabi ma’lumotlarni tiklash harakatlari bilan bog‘liq xarajatlar va vaqtdan qochishadi.

6-rasm. Jismoniy xavfsizlik usb fleshkasi

Jismoniy xavfsizlikning asosiy kamchiligi insoniy jihatdir. Kiberxavfsizlik ma’lumotlari buzilishining 95% inson xatosi natijasidir – jismoniy xavfsizlik choralariga qaramay, zahiraviy axborot vositalarini noto‘g‘ri joylashtirish yoki uni himoyalanmagan holda qoldirish kabi inson xatosi hamon yuz berishi mumkin. Zaxiralangan media joylashuvlarini kuzatib borish va ularni saqlashdan oldin ularning xavfsizligiga ishonch hosil qilish muhim.

Xulosa

Xulosa qilib aytadigan bo‘lsak, ma’lumotlarni himoya qilish bugungi raqamli asrda shaxslar va tashkilotlar uchun muhim masala bo‘lib, fayl safarining barcha

bosqichlarida hal qilinishi kerak. Shifrlash, zaxira nusxasini yaratish va falokatlarni tiklashni rejalashtirish, kirishni boshqarish, tarmoq xavfsizligi va jismoniy xavfsizlikni o‘z ichiga olgan ma’lumotlarni himoya qilishning kompleks yondashuvi nozik ma’lumotlarning xavfsizligi va maxfiyligini ta’minlashga yordam beradi. Texnologiya taraqqiyoti va rivojlanayotgan tahdid landshaftidan xabardor bo‘lish uchun xavfsizlik choralarini muntazam ravishda baholash va yangilash muhimdir.

FOYDALANILGAN ADABIYOTLAR:

1. Wang Zhuo, LIU Guowei, Wang Yan, LI Yuan, Research on the development and trend of data masking technology, November 2020.
2. Raimundas Matulevičius and Henri Lakk, A Model-driven Role-based Access Control for SQL Databases, Complex Systems Informatics and Modeling Quarterly, CSIMQ, Issue 3, July, 2015, Pages 35-62.
3. Ravikumar G K, Dr. B. Justus Rabi, Dr. Ravindra S.Hegadi, Manjunath T.N, Archana R A, “Experimental Study of Various Data Masking Techniques with Random Replacement using data volume”, International Journal of Computer Science and Information Security, Vol. 9, No. 8, August 2011.
4. Emad Khalaf,Mustafa M.K, A Survey of Access Control and Data Encryption for Database Security,Journal of King University Engineering Sciences, 2017.
5. Khin Lay Myint,"Databse Security Model Using Access Control Mechanism in Student Data Management", International journal of Trend in Scientific Research and Developement, april 2019.
6. Ganiyev Salim Karimovich, Karimov Madjit Malikovich, Tashev Komil Axmatovich. Axborot xavfsizligi, Toshkent 2015, 390 b.
7. Ganiev Salim Karimovich, Kuchkarov Taxir Anvarovich. Tarmoq xavfsizligi, Toshkent 2019, 141 b.
8. Ximmatov Ibodilla, Abduraxmanov Muxtor. Axborotni himoyalash, Samarqand 2021, 244 b.
9. Tahirov Behzod Nasriddinovich. Axborot xavfsizligi asoslari, Buxoro 2022, 156 b.