SERVERDAGI MA’LUMOTLARNI HIMOYA QILISH USULLARI

G‘ulomov Sherzod Rajaboyevich
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti. PhD, dotsent.
Ruzimov Omon Narimanovich
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti. Axborot xavfsizligi PhD

Annotatsiya: *Ushbu maqolada serverlarda saqlanadigan ma’lumotlarni yo‘qolishi, buzilishi, o‘g‘irlanishi va kiberhujumlardan himoya qilishning asosiy usullari keltirilgan. Hozirgi kunda ma’lumotlarga qaratilgan hujumlarni himoyalash juda dolzarb masalalardan biri bo‘lib hisoblanganidek, ma’lumotlarni himoya qilish va ularni boshqarish usullari yoritib berilgan.*

Kalit so‘zlar: *Axborot xavfsizligi, kiberxavfsizlik, ma’lumotlar ombori, server, ma’lumotlarni qayta ishlash, shiflash, tarmoq xavfsizligi.*

Kirish: Hozirgi kunda raqamli texnalogiyalar va raqamli ma’lumotlarni qayta ishlash sohalari shiddat bilan rivojlanib bormoqda. Shuningdek, serverdagi ma’lumotlarni himoya qilish, uning infratuzilmasida saqlanadigan maxfiy ma’lumotlarni ruxsatsiz kirish, o‘zgartirish yoki yo‘qotishdan himoya qilish uchun juda muhimdir. Albatta! Serverdagi ma’lumotlarni himoya qilish haqida gap ketganda, xavfsizlikni kuchaytirish uchun bir necha usullardan foydalanish mumkin[1].

Jamiyatda ma’lumotlarni qayta ishlash va ularni himoya qilish O‘zbekiston Respublikasi Konstitutsiyasi, qonunlari, Mehnat kodeksi, qonunosti hujjatlari, ma’lumotlarni qayta ishlash holatlari va xususiyatlarini belgilovchi O‘zbekiston Respublikasining boshqa qonun hujjatlari talablariga muvofiq amalga oshiriladi. O‘zbekiston Respublikasi tegishli organlarining yo‘riqnomalari va uslubiy hujjatlari[2].

Ma’lumotlarni himoya qilish talablari - ma’lumotlarga ishlov berishda Jamiyat ma’lumotlarni ularga noqonuniy va/yoki ruxsatsiz kirishdan, ma’lumotlarni yo‘q qilishdan, o‘zgartirishdan, bloklashdan, nusxalashdan, taqdim etishdan, tarqatishdan, shuningdek, boshqa narsalardan himoya qilish uchun zarur huquqiy, tashkiliy va texnik choralarni ko‘radi[3].

Ma’lumotlar xavfsizligini ta’minlash uchun huquqiy, tashkiliy va texnik choralarni qo‘llash:

1) Shaxsiy ma’lumotlarning axborot tizimlarida qayta ishlash jarayonida ma’lumotlar xavfsizligiga tahdidlarni aniqlash;

2) Ma’lumotlarni himoya qilish talablarini bajarish uchun zarur bo‘lgan shaxsiy ma’lumotlarning axborot tizimlarida qayta ishlash jarayonida ma’lumotlar

xavfsizligini ta’minlash bo‘yicha tashkiliy-texnik chora-tadbirlarni qo‘llash, ularning amalga oshirilishi qonun hujjatlarida belgilangan ma’lumotlar xavfsizligi darajasini ta’minlaydi;

3) Belgilangan tartibda muvofiqlikni baholash tartibidan o‘tgan axborot xavfsizligi vositalaridan foydalanish;

4) Shaxsiy ma’lumotlarning axborot tizimini ishga tushirishdan oldin ma’lumotlar xavfsizligini ta’minlash bo‘yicha ko‘rilgan chora-tadbirlar samaradorligini baholash;

5) Agar ma’lumotlar mashina tashuvchisida saqlangan bo‘lsa, ma’lumotlarning mashina vositalarini hisobga olish;

6) Ma’lumotlarga ruxsatsiz kirish faktlarini aniqlash va kelajakda bunday hodisalarning oldini olish choralarini ko‘rish;

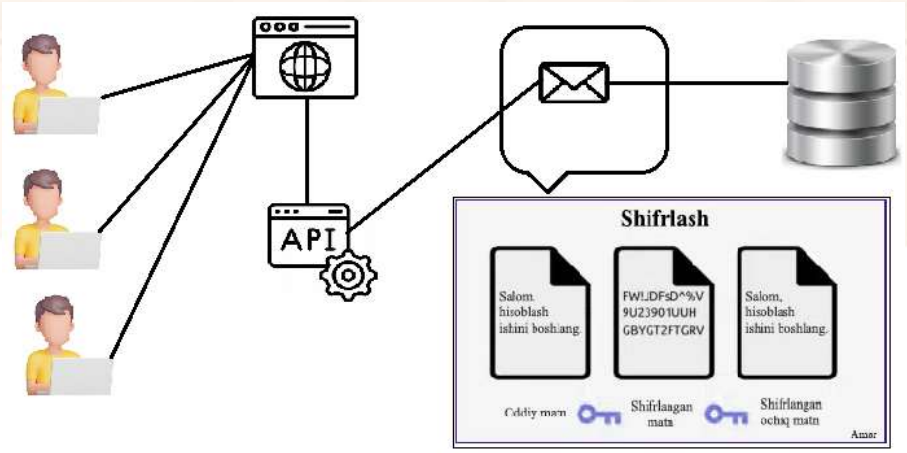
7) Ruxsatsiz kirish natijasida o‘zgartirilgan yoki yo‘q qilingan ma’lumotlarni qayta tiklash;

8) Shaxsiy ma’lumotlarning axborot tizimida qayta ishlangan ma’lumotlarga kirish qoidalarini belgilash, shuningdek, shaxsiy ma’lumotlar tizimidagi ma’lumotlar bilan amalga oshirilgan barcha harakatlarni ro‘yxatdan o‘tkazish va hisobga olishni ta’minlash.

Asosiy qism:

Serverda ma’lumotlarni himoya qilishning ba’zi umumiy usullari:

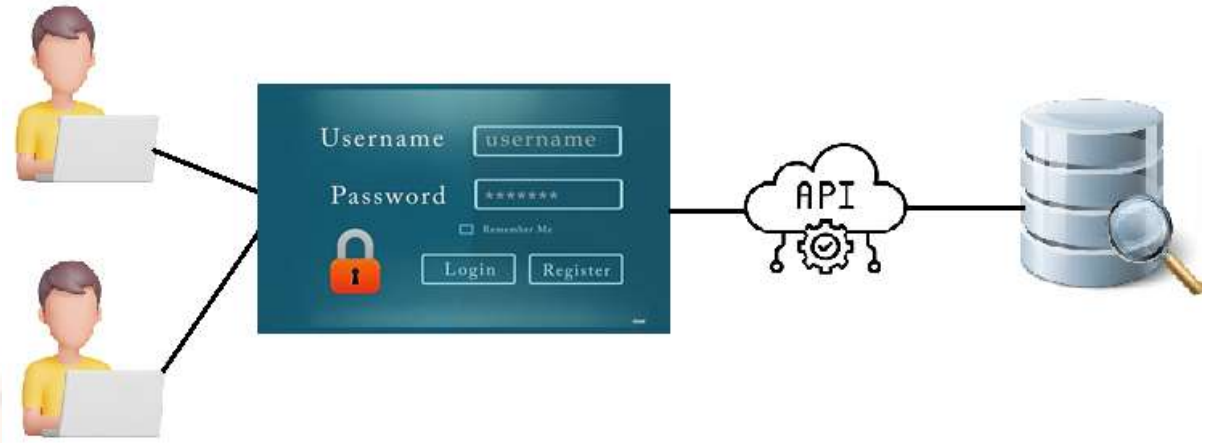
Shifrlash: Ma’lumotni dam olishda ham, uzatishda ham shifrlash juda muhimdir. Tranzitda ma’lumotlarni shifrlash uchun SSL - (Secure Sockets Layer)/TLS - (Transport Level Security) kabi protokollardan, qolgan ma’lumotlarni shifrlash uchun BitLocker yoki LUKS - (Linux Unified Key Setup) kabi texnologiyalardan foydalaning.



1-rasm. Ma’lumotlarni shifrlash

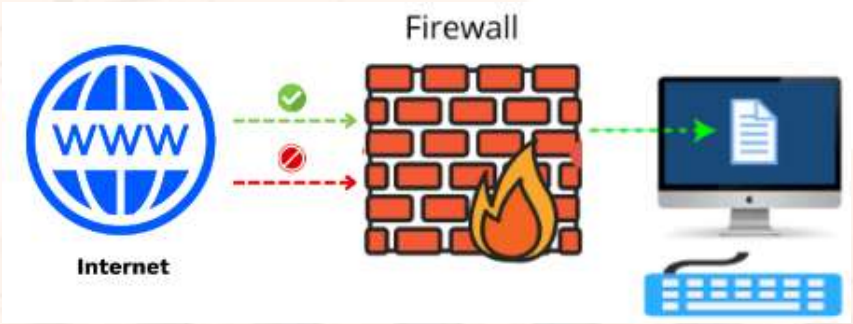
Kirish nazorati: Ma’lumotlarga kim kirishini cheklash uchun kuchli kirish boshqaruvini qo‘llash. Bu rollarga asoslangan ruxsatlarni tayinlaydigan rolga asoslangan kirishni boshqarish (RBAC - Role Based Access Control) kabi usullardan foydalanishni o‘z ichiga oladi va eng kam imtiyoz printsipi,

foydalanuvchilarga o‘z vazifalarini bajarishi uchun zarur bo‘lgan kirishning faqat minimal darajasini beradi.



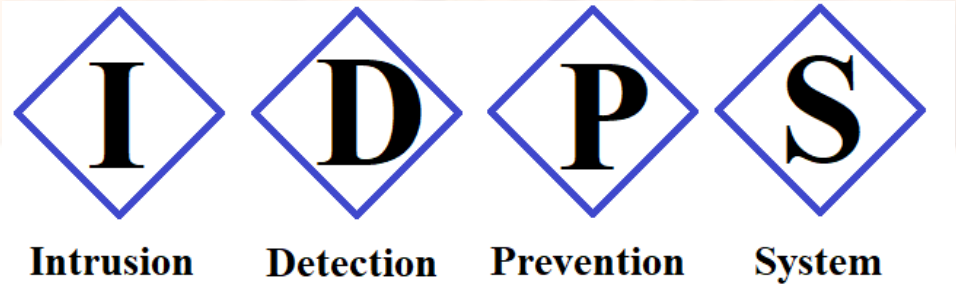
2-rasm. Kirishni nazorat etish

Xavfsizlik devorlari: serverga va serverdan keladigan trafikni boshqarish uchun xavfsizlik devorlarini sozlash. Bu ruxsatsiz kirishning oldini olishga yordam beradi va potentsial zararli trafikni bloklaydi.



3-rasm. Xavfsizlik devorlari (Firewall)

Bosqinni aniqlash va Profilaktika tizimlari (IDPS): IDPS – (Intrusion Detection and Prevention Systems) tarmoq va tizim faoliyatini zararli harakatlar yoki siyosat buzilishi uchun kuzatishi va avtomatik ravishda javob berishi yoki ogohlantirishlar yaratishi mumkin.



4-rasm. Bosqinlarni aniqlash va oldini olish tizimlari (IDPS)

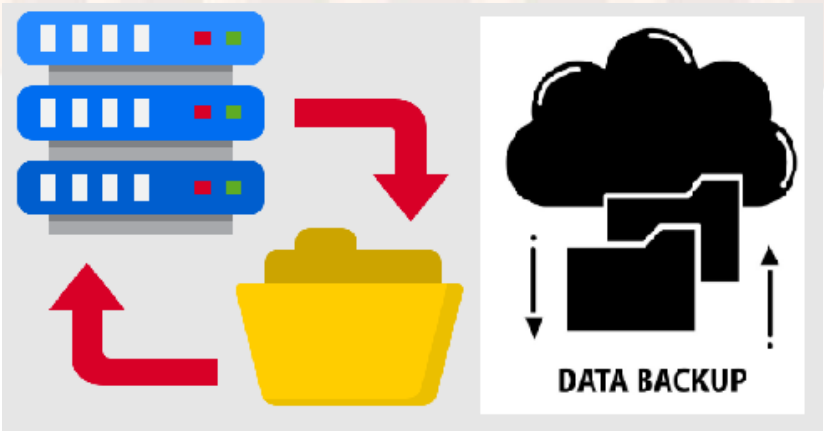
Muntazam yangilanishlar va yamoqlarni boshqarish: ma’lum zaifliklardan foydalanishning oldini olish uchun server dasturlari va operatsion tizimlarini so‘nggi xavfsizlik yamoqlari bilan yangilab turish.

5-rasm. Muntazam yangilanishlar va yamoqlarni boshqarish

Xavfsiz konfiguratsiya: keraksiz xizmatlarni o‘chirib qo‘yish, kuchli parollardan foydalanish va MDH – (CIS - Commonwealth of Independent States) standartlari kabi sanoat standartlarida ko‘rsatilgan eng yaxshi amaliyotlarga rioya qilgan holda xavfsiz konfiguratsiyalarni amalga oshirish orqali serverni xavfsiz sozlang.

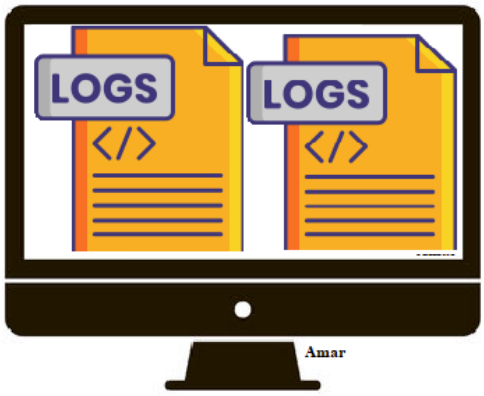
6-rasm. Xavfsiz konfiguratsiya

Ma’lumotlarning zaxira nusxalari: muntazam ravishda ma’lumotlarning zaxira nusxasini yarating va zaxira nusxalari xavfsiz saqlanishini ta’minlang. Bu tasodifiy o‘chirish, buzilish yoki to‘lov dasturi hujumlari tufayli ma’lumotlar yo‘qolgan taqdirda yordam beradi.



7-rasm. Ma’lumotlarning zaxira nusxalari

Monitoring va jurnal: Server faoliyatini kuzatish va shubhali xatti-harakatlarni aniqlash uchun mustahkam jurnalga yozish mexanizmlarini joriy qiling. Ruxsatsiz kirish belgilari yoki boshqa xavfsizlik hodisalari uchun jurnallarni muntazam ravishda tahlil qiling.

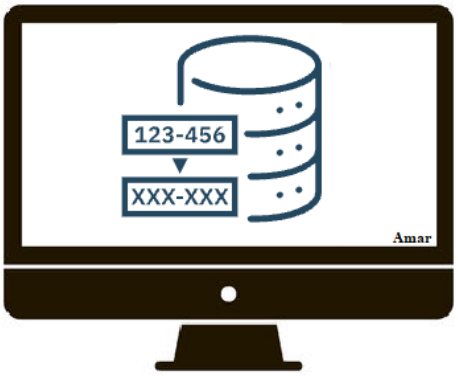


8-rasm. Monitoring va jurnal (Monitoring and Logging)

Ko‘p faktorli autentifikatsiya (MFA - Multi-factor Authentication): Qo‘shimcha xavfsizlik qatlamini qo‘shish uchun foydalanuvchilardan parollar, biometrikalar, smart-kartalar yoki OTP – (One-time password)lar kabi bir nechta omillar yordamida autentifikatsiya qilishni talab qiling.

9-rasm. Ko‘p faktorli autentifikatsiya

Ma’lumotlarni niqoblash va anonimlashtirish: Maxfiy ma’lumotlar uchun maxfiy ma’lumotlarni yashirish yoki xiralashtirish uchun ma’lumotlarni maskalash yoki anonimlashtirish kabi usullarni ko‘rib chiqing.



10-rasm. Ma’lumotlarni niqoblash va anonimlashtirish

Xavfsizlik bo‘yicha trening va xabardorlik: Foydalanuvchilar va ma’murlarni xavfsizlikning eng yaxshi amaliyotlari, jumladan, fishing urinishlarini qanday aniqlash, zararli dasturlardan qochish va ma’lumotlar bilan ishlashning xavfsiz tartib-qoidalariga rioya qilish haqida o‘rgatish.

11-rasm. Xavfsizlik bo‘yicha trening va xabardorlik

Xavfsizlik testi: Xavfsizlikning mumkin bo‘lgan zaif tomonlarini aniqlash va bartaraf etish uchun kirish testi va zaiflikni skanerlash kabi muntazam xavfsizlikni baholashni o‘tkazing.

12-rasm. Xavfsizlik testi (Security Testing)

Xulosa: Xulosa qilib yuqoridagilarni keltirishimiz mumkin. Shuningdek, ushbu usullarni qo‘llash orqali tashkilotlar o‘zlarining serveridagi ma’lumotlarni himoyasini kuchaytirishi va ma’lumotlarning buzilishi, ruxsatsiz kirish undan tashqari boshqa xavfsizlik hodisalari xavfini kamaytirishi mumkin. Doimiy rivojlanib borayotgan tahdidlar muhitida serverlarda ishonchli ma’lumotlarni himoya qilishni ta’minlash uchun faol choralar va doimiy monitoring muhim ahamiyatga ega bo‘ladi.

FOYDALANILGAN ADABIYOTLAR:

1. Ganiev Salim Karimovich, Kuchkarov Taxir Anvarovich. Tarmoq xavfsizligi, Toshkent 2019, 141 b.

2. Ganiyev Salim Karimovich, Karimov Madjit Malikovich, Tashev Komil Axmatovich. Axborot xavfsizligi, Toshkent 2015, 390 b.

3. Narimanovich, R. O. (2024). MA'LUMOTLAR XAVFSIZLIGINI HIMOYA QILISH USULLARI VA TAHLILI. ITALY" ACTUAL PROBLEMS OF SCIENCE AND EDUCATION IN THE FACE OF MODERN CHALLENGES"., 17(1).

4. G'ulomov, S. R. (2023). TARMOQDAGI ZARARLI TRAFIK TURLARI VA ULARNI ANIQLASH. Innovative development in educational activities, 2(24), 424–432. https://doi.org/10.5281/zenodo. 10445437.

5. Ximmatov Ibodilla, Abduraxmanov Muxtor. Axborotni himoyalash, Samarqand 2021, 244 b.

6. «Ахборотлаштириш ва маълумотлар узатиш соҳасида қонунга хилоф ҳаракатлар содир этганлик учун жавобгарлик кучайтирилганлиги муносабати билан Ўзбекистон Республикасининг айрим қонун ҳужжатларига ўзгартиш ва қўшимчалар киритиш тўғрисида» Ўзбекистон Республикасининг қонуни, 25.12.2007 йилдаги №ЗРУ_137-сон.

7. Иргашева Д.Я. Ахборот хавфсизлиги. Тошкент, ТАТУ, 83 б.

8. Зима В. «Безопасность глобальных сетей.» Москва, 2001 г.

9. Брюс Шнайер «Прикладная криптография», М.,2000 г.

10. Александр Вячеславович Фролов. Антивирусная защита: Учебное пособие для защиты информационных ресурсов. 2004 г. http://frolov-lib.ru/books/av/index.html