AXBOROT XAVFSIZLIGINI TA'MINLASH VA DDOS HUJUMLARDAN HIMOYALANISH

B.M.Karajanov
G.D.Amanbayeva
X.A.Alieva
G.B.Alifbayeva
ssistent, Nukus davlat texnika universiteti.
Magistr, Nukus davlat texnika universiteti.
https://doi.org/10.5281/zenodo.15518540

Annotatsiya: Zamonaviy axborot jamiyatida umumiy xavfsizlikning aspektlari, axborot xavfsizligi asosiy masalalardan biridir. Axborot xavfsizligining tarkibiy qismlari maxfiylik, yaxlitlik, mavjudlik, autentifikatsiya va avtorizatsiya, zararli dasturlardan himoyalanish, audit va hatto jismoniy xavfsizlikdir.

Kalit so'zlar: axborot xavfsizligi, maxfiylik, autentifikatsiya, avtorizatsiya, zararli dastur, shifrlash, DDoS hujumlari, simmetrik, asimmetrik.

Axborot xavfsizligi bu ma'lumotlarni ruxsatsiz kirish, yo'q qilish, sizib chiqish yoki ma'lumotlarni o'zgartirish kabi turli tahdid va xavflardan himoya qilish bilan shug'ullanadigan sohadir. Bu haqida ma'lumot himoya qilinishi kerak, shaxsiy ma'lumotlarni o'z ichiga olishi mumkin mijozlar, davlat sirlari, moliyaviy ma'lumotlar va boshqalar.

Axborot xavfsizligining muhim jihatlariga quyidagilar kiradi:

Maxfiylik: ma'lumotlarning maxfiyligini ta'minlash, ya'ni ularga ruxsatsiz kirishning oldini olish.

Butunlik: ma'lumotlarning ruxsatsiz buzilmasligi yoki o'zgartirilmasligi uchun yaxlitligini kafolatlash.

Mavjudlik: ma'lumotlar va axborot resurslari vakolatli foydalanuvchilar uchun kerakli vaqtda mavjud bo'lishini ta'minlash.

Autentifikatsiya va avtorizatsiya: foydalanuvchi identifikatorini tasdiqlash (autentifikatsiya) va ularga kirish huquqlarini boshqarish (avtorizatsiya).

DDoS himoyasi: Tarmoqni ortiqcha yuklash orqali resurslar mavjudligiga hujumlarning oldini oladi.

Shifrlash: ma'lumotlarni shifrlash orqali himoya qilish, ruxsatsiz shaxslarga tushunarsiz qilish [1].

Axborot xavfsizligi tashkilotlar, davlat idoralari va jismoniy shaxslar uchun maxfiy ma'lumotlarning chiqib ketishi va yo'qolishi kabi muhim ahamiyatga ega

ma'lumotlar jiddiy oqibatlarga, shu jumladan moliyaviy yo'qotishlarga olib kelishi mumkin va obro'siga putur etkazadi. Ko'pgina tashkilotlarda alohida

axborot xavfsizligi bo'limlari mavjud va ularning ma'lumotlarini himoya qilish strategiyalarini ishlab chiqadilar.

DDoS hujumlari - tajovuzkorlar juda ko'p sonli so'rovlarni yaratish orqali veb-resurs yoki tarmoqni ortiqcha yuklashga harakat qiladigan tarkibiy qism. DDoS hujumlaridan himoya qilish turli strategiyalarni va bularning oqibatlarini oldini olish yoki yumshatishga qaratilgan texnologiyalar hisoblanadi. Bunga trafikni filtrlash, CDN-lardan foydalanish (kontentni etkazib berish tarmoqlari), foydalanuvchi xatti-harakatlarini tahlil qilish va veb-resursning barqaror ishlashini ta'minlashning boshqa usullari kiradi [2].

DDoS hujumlaridan himoya qilish turli usullar va texnologiyalarni o'z ichiga oladi, bunday hujumlarning oldini olish yoki ta'sirini yumshatish uchun mo'ljallangan.

DDoS hujumlaridan himoya qilishning asosiy usullaridan ba'zilari:

Trafikni filtrlash: Himoya qilishning eng keng tarqalgan usullaridan biri bu trafikni filtrlash vositalaridan foydalanishdir. Bunga IP filtrlash, ma'lum bo'lgan zararli IP manzillarni bloklash va anomal trafikni aniqlash vositalaridan foydalanish kiradi.

CDN (Content Delivery Network) dan foydalanish: CDNlar yetkazib berish tarmoqlari turli serverlar va mavjud geografik nuqtalar o'rtasida yukni taqsimlovchidir. Ular yukni kamaytirishga yordam beradi asosiy server va kontentni yetkazib berish tezligini oshirishadi.

Yukni muvozanatlash: yuk balansidan foydalanish imkonini beradi so'rovlarni bir nechta serverlar bo'ylab teng ravishda taqsimlash, DDoS hujumlari qilish unchalik samarali emas.

Proksi-serverlar: filtrlash uchun proksi-serverlardan foydalanish mumkin trafik va serverning haqiqiy IP manzilini yashirish. Bulutli echimlar: Ba'zi bulutli provayderlar DDoS himoyasi xizmatlarini taqdim etadilar, bu erda ular hujumlardan oldin ularni hal qilishlari mumkin.

Kuchni tekshirish: muntazam ravishda kuch sinovlarini o'tkazish zaifliklarni aniqlash va xavfsizlik tizimini yaxshilash imkonini beradi.

DDoS hujumlaridan himoya qilish murakkab va doimiy o'zgaruvchan jarayon ekanligini tushunish muhimdir. Hujumchilar doimiy ravishda hujumlarni amalga oshirishning yangi usullarini topadilar, shuning uchun veb-resursning barqaror ishlashini ta'minlash uchun xavfsizlik usullarini doimiy ravishda yangilash va takomillashtirish zarur[3].

Axborotni taqdim etishda shifrlash usullari muhim rol o'ynaydi xavfsizlik. Shifrlash maxfiylikni himoya qilish uchun ishlatiladi.

Zamonaviy axborot xavfsizligi tizimlarida keng qo'llaniladigan bir nechta shifrlash usullari:

Simmetrik shifrlash: Bu usul ma'lumotlarni shifrlash va shifrini ochish uchun bitta kalitdan foydalanadi. Biroq, simmetrik shifrlash bilan bog'liq muammo shundaki, aloqaning ikkala tomoni ham kalitga kirish huquqiga ega bo'lishi kerak, bu kalitni uzatishda xavfsizlikka xavf tug'dirishi mumkin.

Asimmetrik shifrlash: Bu usul umumiy va shaxsiy kalit juftligini ishlatadi. Ochiq kalit ma'lumotlarni shifrlash uchun, shaxsiy kalit esa uni ochish uchun ishlatiladi. Bu kalitlarni taqsimlash bilan bog'liq xavfsizlik xatarlarini yo'q qiladi va uni simmetrik shifrlashdan ko'ra xavfsizroq qiladi.

Xeshlash: Ushbu usul ma'lumotlarning yaxlitligini ta'minlash uchun ishlatiladi. Asl ma'lumotlardagi har qanday kichik o'zgarish xesh summasining sezilarli o'zgarishiga olib keladi va bu ma'lumotlar yaxlitligini tekshirish uchun foydali bo'ladi.

Kalit almashish protokollari: Bu protokollar xavfsiz ishlash va aloqada ishtirok etuvchi tomonlar o'rtasida shifrlash kalitlarini almashish uchun ishlatiladi. Bunday protokollarga Diffie-Hellman va RSA protokollarini misol qilib keltirish mumkin.

Fayl va disk darajasida shifrlash: Bu usul himoya qilish uchun ishlatiladi,va bunda fayl va disk darajasidagi ma'lumotlar, ularning maxfiyligi va yaxlitligini ta'minlanadi. Masalan, Windows uchun BitLocker va macOS uchun FileVault.

SSL/TLS protokollari: Ushbu protokollar ma'lumotlarni himoya qilish uchun ishlatiladi. Ular mijoz va server o'rtasida ma'lumotlarni shifrlashni ta'minlaydi, ma'lumotlarni tajovuzkorlar tomonidan ushlab qolishdan himoya qiladi[4].

Axborot xavfsizligiga oid maxsus talablar va har bir usul bilan bog'liq bo'lishi mumkin bo'lgan zaifliklar va xavflarni hisobga olishga qarab tegishli shifrlash usulini tanlash muhimdir

Adabiyotlar ro'yxati:

1. Гродзенский Я.С. Информационная безопасность / Я.С. Гродзенский. – М.:РГ-Пресс, 2023. – 144 с.

2. Басканов А.Н. Способы противодействия и средства раннего выявления DDoS-атак / А.Н. Басканов // Экономика и качество систем связи. – 2019 [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru (дата обращения: 24.10.2023).

3. Титов Ф.М. Исследование методов защиты от атаки DDOS / Ф.М. Титов//Научные междисциплинарные исследования: сборник материалов II Международной научно-практической конференции 1993. -278 с.

4. Li.Z, Iyer.R, Makineni.S. “Anatomy and Performance of SSL” Processing. Proceedings of the IEEE International Symposium on Performance Analysis of Systems and Software.2005: 197- 206