TO‘LOV TIZIMLARIDA XAVFSIZLIK MUAMMOLARI VA TAHDIDLAR

Saidov Ozodbek Alisher o‘g‘li
Normamatov Xusan Baxodir o‘g‘li
Seytmamatov Sohibjon Muzaffar o‘g‘li
TATU, Kiberxavfsizlik fakulteti talabalari
Saburova Shoxista Shavkat qizi

Annotatsiya: *Mazkur maqolada to‘lov tizimlarida uchraydigan asosiy xavfsizlik muammolari va kiberxavflar tahlil qilinadi. Tadqiqot davomida phishing, ransomware, DDoS hujumlari, malware, ma’lumotlar sizib chiqishi hamda ijtimoiy muhandislik kabi tahdidlarning ishlash mexanizmlari va ularning moliyaviy tizimlarga ta’siri o‘rganilgan. Shuningdek, autentifikatsiya, shifrlash, ko‘p faktorli himoya va zamonaviy xavfsizlik texnologiyalarining ahamiyati yoritilgan. Tadqiqot natijalari to‘lov tizimlarida axborot xavfsizligini ta’minlash moliyaviy barqarorlik va foydalanuvchilar ishonchini saqlashda muhim omil ekanligini ko‘rsatadi.*

Kalit so‘zlar: *To‘lov tizimlari, axborot xavfsizligi, phishing, ransomware, DDoS hujumlari, malware, data breach, kiberxavfsizlik, autentifikatsiya, shifrlash, elektron to‘lovlar, ijtimoiy muhandislik, bank xavfsizligi, moliyaviy firibgarlik.*

To‘lov tizimlarida xavfsizlik masalasi zamonaviy raqamli iqtisodiyotning eng dolzarb yo‘nalishlaridan biri hisoblanadi. Moliyaviy operatsiyalarning katta qismi elektron shaklga o‘tgani sari, ushbu tizimlar kiberjinoyatchilar uchun yanada jozibador nishonga aylanmoqda. To‘lov tizimlari orqali nafaqat pul mablag‘lari, balki foydalanuvchilarning shaxsiy va moliyaviy ma’lumotlari ham qayta ishlanadi. Shu sababli bu tizimlarga qaratilgan har qanday hujum keng ko‘lamli iqtisodiy zarar, foydalanuvchilar ishonchining pasayishi va moliyaviy barqarorlikka tahdid tug‘dirishi mumkin.

To‘lov tizimlarida xavfsizlik tushunchasi odatda ma’lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta’minlash bilan bog‘liq bo‘ladi. Maxfiylik foydalanuvchi ma’lumotlarining begona shaxslar tomonidan o‘qilmasligini anglatadi, yaxlitlik ma’lumotlarning o‘zgarmagan holda saqlanishini, mavjudlik esa tizim xizmatlarining uzluksiz ishlashini ta’minlaydi. Ushbu uchta asosiy prinsipga amal qilinmagan holatlarda turli xil kiberxavfsizlik muammolari yuzaga keladi.

So‘nggi yillarda to‘lov tizimlariga qarshi amalga oshirilayotgan kiberhujumlar soni va murakkabligi keskin oshgan. Bunga bir tomondan raqamli texnologiyalarning tez rivojlanishi sabab bo‘lsa, boshqa tomondan hujumchilarning texnik imkoniyatlari va tajribasi ham ortib bormoqda. Kiberjinoyatchilar an’anaviy hujum usullaridan tashqari sun’iy intellekt, avtomatlashtirilgan skriptlar va ijtimoiy muhandislik usullaridan keng foydalanmoqda.

To‘lov tizimlarida eng ko‘p uchraydigan tahdidlardan biri phishing hujumlaridir. Ushbu usulda foydalanuvchi aldov yo‘li bilan o‘zining login, parol, bank karta rekvizitlari yoki bir martalik tasdiqlash kodlarini hujumchiga berib qo‘yadi. Phishing hujumlari

ko‘pincha bank nomidan yuborilgan soxta xabarlar, elektron pochta yoki veb-sahifalar orqali amalga oshiriladi. Foydalanuvchi asl tizimga o‘xshash soxta sahifaga kirib, o‘z ma’lumotlarini kiritadi va natijada ushbu ma’lumotlar hujumchilar qo‘liga tushadi.

Zararli dasturlar ham to‘lov tizimlari xavfsizligiga jiddiy tahdid soladi. Banking trojanlar foydalanuvchining qurilmasiga yashirin tarzda o‘rnatilib, klaviaturadan kiritilgan ma’lumotlarni yozib olishi, ekran tasvirlarini saqlashi yoki to‘g‘ridan-to‘g‘ri bank ilovalariga aralashishi mumkin. Ba’zi zararli dasturlar tranzaksiyalarni o‘zgartirib yuborishga ham qodir bo‘lib, foydalanuvchi sezmagan holda mablag‘lar boshqa hisob raqamiga o‘tkaziladi.

Man-in-the-Middle hujumlari ham keng tarqalgan bo‘lib, bunda hujumchi foydalanuvchi va server o‘rtasidagi aloqani nazorat ostiga oladi. Bunday hujumlar ko‘pincha himoyalanmagan tarmoqlar, masalan, ochiq Wi-Fi orqali amalga oshiriladi. Natijada yuborilayotgan ma’lumotlar o‘qib olinishi yoki o‘zgartirilishi mumkin. Bu esa ayniqsa onlayn to‘lovlar vaqtida katta xavf tug‘diradi.

To‘lov tizimlariga qarshi amalga oshiriladigan yana bir muhim hujum turi xizmatdan voz kechishga majbur qilish, ya’ni DDoS hujumlaridir. Bunday hujumlar orqali tizimga juda ko‘p so‘rov yuborilib, uning ishlashi izdan chiqariladi. Natijada foydalanuvchilar xizmatlardan foydalana olmaydi, bu esa banklar va to‘lov operatorlari uchun katta moliyaviy va reputatsion zarar keltiradi.

Kartaga asoslangan to‘lov tizimlarida esa skimming deb ataluvchi usul keng uchraydi. Bu usulda maxsus qurilmalar yordamida bank kartasining magnit tasmasidan ma’lumotlar o‘qib olinadi va PIN-kodlar yozib olinadi. Keyinchalik ushbu ma’lumotlar asosida kartaning nusxasi tayyorlanib, noqonuniy operatsiyalar amalga oshiriladi.

To‘lov tizimlaridagi zaifliklar ko‘pincha texnik kamchiliklar yoki noto‘g‘ri sozlamalar bilan bog‘liq bo‘ladi. Masalan, autentifikatsiya tizimlarining zaifligi foydalanuvchi hisobining osonlik bilan buzilishiga olib keladi. Oddiy parollar, bir xil parollardan foydalanish yoki ikki faktorli autentifikatsiyaning yo‘qligi xavfni oshiradi. Tarmoq darajasidagi zaifliklar, jumladan shifrlanmagan ma’lumot uzatish yoki noto‘g‘ri konfiguratsiya qilingan serverlar ham hujumchilarga imkon yaratadi.

Zamonaviy to‘lov tizimlarida keng qo‘llaniladigan API interfeyslari ham xavfsizlik nuqtai nazaridan muhim hisoblanadi. Agar API lar to‘g‘ri himoyalanmagan bo‘lsa, hujumchilar ular orqali tizimga kirib, ma’lumotlarni o‘zgartirishi yoki o‘g‘irlashi mumkin. Autentifikatsiya va avtorizatsiya mexanizmlaridagi xatolar, tokenlarni noto‘g‘ri boshqarish va so‘rovlarni tekshirishning yetarli emasligi bunday zaifliklarga sabab bo‘ladi.

Inson omili esa to‘lov tizimlaridagi eng katta xavflardan biri hisoblanadi. Foydalanuvchilarning ehtiyotsizligi, xodimlarning xatolari yoki yetarli darajada bilimga ega emasligi ko‘plab kiberhujumlarning muvaffaqiyatli amalga oshishiga sabab bo‘ladi. Ijtimoiy muhandislik usullari aynan inson psixologiyasiga ta’sir qilish orqali ma’lumotlarni qo‘lga kiritishga qaratilgan.

Moliyaviy firibgarlik sxemalari ham to‘lov tizimlarining ajralmas muammolaridan biridir. Hisobni egallab olish holatlarida foydalanuvchining login va paroli o‘g‘irlanadi va hujumchi uning nomidan operatsiyalarni amalga oshiradi. SIM kartani almashtirish orqali

SMS tasdiqlash kodlarini qo‘lga kiritish usuli ham keng tarqalgan. Bundan tashqari, soxta to‘lovlar, ya’ni pul o‘tkazilgandek ko‘rsatib foyda olish, yoki to‘lov amalga oshirilgandan keyin uni bekor qilish orqali firibgarlik qilish holatlari ham mavjud.

Amaliyotda kuzatilgan yirik kiberhujumlar to‘lov tizimlarining zaif tomonlarini yaqqol namoyon etadi. Masalan, banklararo to‘lov tizimiga noqonuniy kirish orqali millionlab dollar mablag‘lar o‘g‘irlangan holatlar qayd etilgan. Ayrim hollarda savdo tarmoqlarining to‘lov terminallariga zararli dasturlar o‘rnatilib, millionlab bank kartalari ma’lumotlari qo‘lga kiritilgan. Bunday hodisalar nafaqat moliyaviy zarar, balki mijozlar ishonchining keskin pasayishiga ham olib keladi.

Statistik ma’lumotlar shuni ko‘rsatadiki, to‘lov tizimlariga qarshi kiberhujumlar soni yil sayin ortib bormoqda. Ayniqsa mobil to‘lov tizimlari va elektron tijorat platformalari eng ko‘p nishonga olinayotgan sohalardan biri hisoblanadi. Kiberjinoyatchilar tomonidan qo‘llanilayotgan usullar tobora murakkablashib borayotgani esa ushbu muammoning dolzarbligini yanada oshirmoqda.

To‘lov tizimlaridagi xavfsizlik muammolarining oqibatlari juda jiddiy bo‘lishi mumkin. Moliyaviy yo‘qotishlar bilan bir qatorda, tashkilotlar o‘z obro‘siga putur yetkazadi, mijozlar ishonchini yo‘qotadi va ko‘pincha huquqiy javobgarlikka tortiladi. Shu sababli xavfsizlikni ta’minlash nafaqat texnik masala, balki strategik muhim vazifa sifatida qaralishi lozim.

Umuman olganda, ushbu bobda to‘lov tizimlarida mavjud bo‘lgan asosiy xavfsizlik muammolari, tahdidlar va zaifliklar keng qamrovda tahlil qilindi. Tahlillar shuni ko‘rsatadiki, zamonaviy to‘lov tizimlari yuqori texnologik darajaga ega bo‘lishiga qaramay, ular turli xil kiberxavflarga duch kelmoqda. Shu sababli keyingi bobda ushbu muammolarni bartaraf etish yo‘llari, zamonaviy himoya texnologiyalari va xavfsizlikni kuchaytirish mexanizmlari batafsil yoritiladi.

Kiberxavflarning eng keng tarqalgan turlaridan biri bu *phishing* hisoblanadi. Phishing hujumlari foydalanuvchilardan maxfiy ma’lumotlarni, masalan, login va parollarni, bank kartasi rekvizitlarini yoki boshqa shaxsiy ma’lumotlarni qo‘lga kiritishga qaratilgan bo‘ladi. Bunda hujumchilar o‘zlarini ishonchli tashkilot yoki shaxs sifatida ko‘rsatib, elektron pochta, ijtimoiy tarmoqlar yoki soxta veb-saytlar orqali foydalanuvchini aldashga harakat qiladi. Phishing hujumlari ko‘pincha inson omiliga asoslangan bo‘lib, texnik himoya vositalaridan ko‘ra foydalanuvchilarning ehtiyotsizligidan foydalanadi.

Yana bir xavfli kiberxavf turi bu *ransomware* hisoblanadi. Ransomware – bu zararli dastur bo‘lib, u tizimga kirgandan so‘ng foydalanuvchining ma’lumotlarini shifrlab qo‘yadi va ularni qayta tiklash uchun ma’lum miqdorda pul talab qiladi. Ko‘pincha bunday hujumlar tashkilotlar uchun katta moliyaviy yo‘qotishlarga olib keladi, chunki muhim ma’lumotlarga kirish imkoniyati vaqtincha yoki butunlay yo‘qolishi mumkin. Ransomware hujumlari odatda phishing orqali yoki zaifliklardan foydalanish orqali tizimga kiradi.

Kiberxavflarning yana bir muhim turi bu *DDoS (Distributed Denial of Service)* hujumlaridir. DDoS hujumlari server yoki tarmoq resurslarini haddan tashqari yuklab, uni foydalanuvchilar uchun mavjud bo‘lmaydigan holatga keltirishga qaratilgan. Bunda ko‘plab qurilmalar (botnet) bir vaqtning o‘zida maqsadli serverga so‘rov yuboradi. Natijada tizim

ishlamay qoladi yoki juda sekin ishlaydi. Bu esa ayniqsa onlayn xizmatlar ko‘rsatuvchi kompaniyalar uchun jiddiy muammolarni keltirib chiqaradi.

Bundan tashqari, *malware (zararli dasturlar)* ham keng tarqalgan kiberxavflardan biridir. Malware tushunchasi viruslar, trojanlar, spyware va boshqa zararli dasturlarni o‘z ichiga oladi. Ular tizimga zarar yetkazish, ma’lumotlarni o‘g‘irlash yoki foydalanuvchini kuzatish maqsadida yaratiladi. Malware ko‘pincha zararli fayllar, noma’lum havolalar yoki shubhali dasturlar orqali tizimga kiradi.

Shuningdek, *ma’lumotlar sizib chiqishi (data breach)* ham zamonaviy kiberxavflarning muhim turlaridan biri hisoblanadi. Bunday holatda maxfiy yoki muhim ma’lumotlar ruxsatsiz shaxslar qo‘liga tushadi. Bu esa kompaniyaning obro‘siga putur yetkazishi, moliyaviy zarar keltirishi va hatto huquqiy javobgarlikka olib kelishi mumkin.

Yana bir keng tarqalgan tahdid bu *ijtimoiy muhandislik (social engineering)* hujumlaridir. Bu usulda hujumchilar texnik zaifliklardan emas, balki inson psixologiyasidan foydalanadi. Masalan, foydalanuvchini aldash, qo‘rqitish yoki ishonchiga kirish orqali maxfiy ma’lumotlarni olishga harakat qilinadi.

Zararli xabarlar foydalanuvchiga tanish ko‘rinishi mumkin, shuning uchun har doim ehtiyotkorlik bilan ochish va ishonchli manbadan kelganiga ishonch hosil qilish zarur.

2.1-rasm. Phishing (aldov orqali ma’lumot o‘g‘irlash)

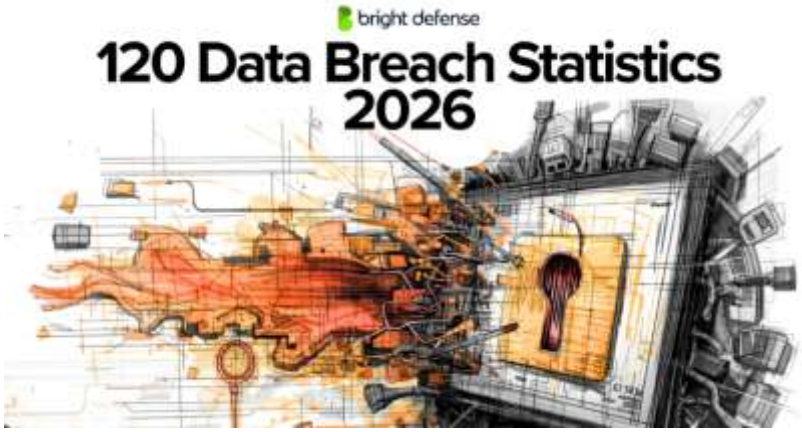
DDoS hujumlari

DDoS (Distributed Denial of Service) hujumlari tizim serverlariga juda katta hajmdagi so‘rovlar yuborish orqali ularni ishdan chiqarishga qaratilgan. Bunday hujum natijasida platforma vaqtincha ishlamay qoladi, foydalanuvchilar auktsionda ishtirok eta olmaydi va savdo jarayoni to‘xtab qoladi. Bu esa katta moliyaviy va reputatsion zarar keltiradi.

2.2-rasm. DDoS hujumlari

Ma’lumotlar sizib chiqishi (Data breach)

Onlayn auktsion platformalarida foydalanuvchilarning shaxsiy va moliyaviy ma’lumotlari saqlanadi. Agar tizimda xavfsizlik yetarli darajada ta’minlanmagan bo‘lsa, hujumchilar ushbu ma’lumotlarni o‘g‘irlashi mumkin. Bu esa foydalanuvchilarning maxfiyligi buzilishiga va ularning ishonchi yo‘qolishiga olib keladi.



2.3-rasm. Ma’lumotlar sizib chiqishi (Data breach)

Zararli dasturlar (Malware)

Zararli dasturlar foydalanuvchilarning qurilmasiga yoki platforma serverlariga zarar yetkazish maqsadida ishlatiladi. Masalan, ayrim dasturlar foydalanuvchining klaviaturada kiritgan ma’lumotlarini yozib oladi va firibgarlarga yuboradi. Natijada login, parol va bank ma’lumotlari o‘g‘irlanishi mumkin.