KOMPYUTER TARMOQLARIDA TARMOQ HUJUMLARI IZLARINI ANIQLASH MODELLARI VA ALGORITMLARI

G‘ulomov Sherzod Radjaboyevich
Muxammad al – Xorazmiy nomidagi TATU “Kiberxavfsizlik” fakulteti dekani, dotsent, tel:+998909708464
Ramazonova Madina Shavkatovna
Muxammad al – Xorazmiy nomidagi TATU “Kiberxavfsizlik va kriminalistika” kafedrasi assistenti, tel:+998997481489

Hozirgi kunda kompyuter tarmoqlari bizning kundalik hayotimizda muhim rol o'ynamoqda, ular biznes jarayonlaridan tortib, shaxsiy ma'lumotlar almashinuvi va kommunikatsiyagacha keng ko'lamli xizmatlarni taqdim etadi. Biroq, tarmoq infratuzilmasining kengayishi va murakkabligi bilan birga, tarmoq xavfsizligi masalalari ham jiddiy ahamiyatga ega bo'lmoqda. Har yili millionlab tarmoq hujumlari ro'y berishi, ma'lumotlarni o'g'irlash, xizmatni rad etish (DoS) va boshqa xavf-xatarlar keltirib chiqarishi mumkin. Statistika ma'lumotlariga ko'ra, 2023-yilda tarmoq xavfsizligiga tahdidlar 60% ga oshdi, bu esa tashkilotlarni yanada samarali xavfsizlik choralarini ko'rishga undamoqda.

Tarmoq hujumlarini aniqlash tizimlari (IDS) xavfsizlikni ta'minlashda muhim vositalardan biridir. Ular tarmoq trafigini monitoring qilish, anomal faoliyatni aniqlash va tahdidlarni oldini olishga qaratilgan. Ushbu maqola tarmoq hujumlarini aniqlashda qo'llaniladigan modellarning va algoritmlarning xilma-xilligini ko'rib chiqadi. Qoidaga asoslangan, statistik va mashinani o'rganish yondashuvlari kabi turli usullarni tahlil qilib, ularning samaradorligi va qiyinchiliklari belgilab olinadi.

Quyidagi omillar hozirda tarmoq muammolarining ko'payishiga yordam beradi:

Qurilma yoki dasturiy ta'minot vositasi to'g'ri sozlanmagan. Xavfsizlik zaifliklari odatda tarmoqdagi qurilma yoki dasturiy ta'minotni noto'g'ri sozlash natijasida yuzaga keladi. Masalan, noto'g'ri tuzilgan yoki shifrlanmagan protokoldan foydalanish tarmoq orqali yuborilgan maxfiy ma'lumotlarni oshkor qilishga olib keladi. Noto'g'ri sozlangan qurilma tajovuzkorga tizim yoki tarmoqqa kirish huquqini berishi mumkin. Noto'g'ri sozlangan dasturiy ta'minot vositasi dastur yoki dasturiy ta'minotdan ruxsatsiz foydalanishga olib kelishi mumkin.

Xavfli va yomon tarmoq dizayni. Noto'g'ri va xavfli tarzda ishlab chiqilgan tarmoq turli xil tahdidlarga va ma'lumotlarni yo'qotish ehtimoliga duch kelishi mumkin. Misol uchun, agar xavfsizlik devori, IDS va virtual xususiy tarmoq (VPN) texnologiyalari xavfsiz tarzda amalga oshirilmasa, ular tarmoqni turli tahdidlarga qarshi himoyasiz qoldirishi mumkin.

Tug'ma texnologik zaiflik. Agar qurilma yoki dasturiy ta'minot vositasi tarmoq hujumlarining ayrim turlariga dosh berolmasa, u ushbu hujumlarga qarshi himoyasiz bo'ladi. Ko'pgina qurilmalar, ilovalar yoki veb-brauzerlar ularni xizmatdan voz kechishga undaydigan hujumga yoki shaxsning hujumlariga toqat qilmaydilar. Agar tizimlar eski veb-brauzerdan foydalansa, bu tizimlar tarqatilgan hujumlarga nisbatan zaifroq bo'ladi. Agar

tizimlar yangilanmagan bo'lsa, foydalanuvchi mashinasini tozalash uchun kichik troyan hujumi etarli bo'lishi mumkin.

Foydalanuvchilarning bexabarligi. So'nggi tarmoq foydalanuvchilarining beparvoligi tarmoq xavfsizligiga katta ta'sir ko'rsatishi mumkin. Ma'lumotlarning yo'qolishi, inson xatti-harakatlari natijasida oqish kabi jiddiy xavfsizlik muammolari paydo bo'lishi mumkin. Hujumchilar, shuningdek, foydalanuvchilar haqida ma'lumot to'plash uchun ijtimoiy muhandislik texnologiyalaridan foydalanadilar.

Foydalanuvchilarning qasddan harakatlari. Ishdan bo'shatilgan xodim hali ham tarqatilgan diskdan foydalanishi mumkin. Bunday holda, bu tashkilotning maxfiy ma'lumotlari sizib chiqishiga olib keladi. Bu holat foydalanuvchilarning qasddan qilgan harakatlari sifatida qabul qilinadi.

Tarmoq tahdidlari odatda ikki turga bo'linadi: ichki tahdidlar va tashqi tahdidlar.

Ichki tahdidlar. Kompyuter yoki Internet bilan bog'liq jinoyatlarning 80% ichki hujumlardir. Ushbu hujumlar tashkilot ichidagi xafa bo'lgan, zararli xodimlar tomonidan amalga oshirilishi mumkin. Ushbu hujumlarning aksariyati imtiyozli tarmoq foydalanuvchilari tomonidan amalga oshiriladi.

Ichki hujumlar tashqi hujumlarga qaraganda jiddiyroq tahdid solishi mumkin.

Asosiy buning sababi ichki hujumni amalga oshiradigan tarmoqning qulashi, xavfsizlik siyosati va tashkilotning qonunchilikni bilishi.

Tashqi tahdidlar. Tashqi hujumlar tarmoqdagi allaqachon mavjud bo'lgan zaiflikning natijasidir. Hujumchi ushbu hujumlarni shunchaki qiziqish, moddiy manfaat yoki tashkilotni obro'sizlantirish uchun amalga oshirishi mumkin. Shu bilan birga, hujumchi yuqori malakaga ega va jamoada ishlashi mumkin. Hujum paytida maxsus texnologiyalar qo'llaniladi, uzoq muddatli tayyorlik kuzatiladi. Bunday holda, hujumlar ichki xodimlarning yordamisiz amalga oshiriladi. Ba'zi tashqi hujumlarga tajovuzkorlar va viruslarga asoslangan hujumlar, parollarga asoslangan hujumlar, zararli xabarlarga asoslangan hujumlar va operatsion tizimga asoslangan hujumlar kiradi.

Tashqi tahdidlar odatda ikki turga bo'linadi: tuzilgan va tizimsiz tashqi tahdidlar.

Tizimlashtirilgan tashqi tahdid. Tizimlashtirilgan tashqi tahdidlar yuqori malakali shaxslar tomonidan amalga oshiriladi. Bu odamlar tarmoqdagi mavjud zaiflikni tezda aniqlay olishadi va undan o'z manfaatlari yo'lida foydalanishlari mumkin. Ushbu shaxslar yoki shaxslar guruhlari odatda yirik kiber jinoyatlar bilan shug'ullanadilar.

Tizimsiz tashqi tahdid. Tizimsiz tashqi tahdidlar odatda malakasiz shaxslar tomonidan turli xil tayyor xakerlik vositalari va skriptlardan foydalangan holda amalga oshiriladi. Ushbu turdagi hujumlar odatda shaxslar tomonidan o'z qobiliyatlarini sinab ko'rish yoki tashkilotda zaiflik mavjudligini tekshirish uchun amalga oshiriladi.

Antivirus dasturidan qanday foydalanish kerak:

Antivirus dasturi qurilmangizni ma'lumotlarni o'chirib tashlaydigan, qurilmangizni sekinlashtiradigan yoki o'chiradigan yoki spamerlarga hisobingiz orqali elektron pochta xabarlarini yuborishga imkon beradigan viruslardan himoya qiladi. Antivirus himoyasi fayllarni va keraksiz elektron pochta xabarlarini viruslarni tekshiradi va keyin zararli narsalarni olib tashlaydi. Internetda tarqalgan so'nggi "xatolar" bilan kurashish uchun

antivirus dasturini doimiy ravishda yangilab turishingiz kerak. Ko'pgina antivirus dasturlari internetda bo'lganingizda yangilanishlarni avtomatik ravishda yuklab olish imkoniyatiga ega. Bundan tashqari, dasturiy ta'minot doimiy ravishda ishlayotganiga va tizimni viruslarni tekshirayotganiga ishonch hosil qiling, ayniqsa internetdan fayllarni yuklab olayotgan bo'lsangiz yoki elektron pochtangizni tekshirayotgan bo'lsangiz. Viruslarni har kuni skanerlash uchun antivirus dasturini o'rnating. Bundan tashqari, tizimingizni oyiga kamida ikki marta yaxshilab skanerlashingiz kerak.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

1. Anorboyev A. Kiberjinoyatchilik jinoyati: jinoiy-huquqiy va kriminologik tavsiflar. - T.: 2020, huquqiy tadqiqotlar jurnali. 2-maxsus raqam. B. 300309.

2. Turdiyeva G. S., Shalimov A. S. Ka'lim tizimida zamonaviy bulutli xizmatlardan foydalanishning asosiy xususiyatlari va funktsiyalari// fan va ta'lim Byulleteni 2021. № 17 (120).3-qism. 52-55 sahifalar

3. Durdiyeva G. S. Kurizm sohasida axborot texnologiyalaridan foydalanish / / Shoyimov A. "akademiya" ilmiy-uslubiy jurnali Rossiya-ta'sir omili: 0.19. №6 (57). 2020 yil 22-24 bet.