6 – TOM 5 – SON / 2023 - YIL / 15 - MAY

ISHCHI STANSIYA VA SERVER TUZILMASIDA ZAIFLIKLARNI ANIQLASH JARAYONI

Bozorova Feruza Xaydar qizi
Toshkent axborot texnologiyalari universiteti
Axborot xavfsizligi kafedrasi, 2-kurs magistranti,
Odilov Ilhom Isoq o‘g‘li
Toshkent axborot texnologiyalari universiteti
Axborot xavfsizligi kafedrasi, 2-kurs magistranti,

Annotatsiya: *Mazkur maqolada ishchi stansiya va server tuzilmasida zaifliklarni aniqlash jarayoni haqida so‘z yuritiladi.*

Kalit so‘zlar: *Axborot texnologiyalari sohasidagi jinoyatlar, elektron jinoyatlar, kompyuter jinoyatlari, kiberjinoyatlar, xavfsizlik devori.*

Hozirgi kunda axborot texnologiyalarining jadal rivojlanishi va kishilik jamiyatining barcha sohalarida internetdan keng foydalanish kundalik faoliyatning bir qismini tashkil etib, xizmat ko‘rsatish, ilm-fan, ta’lim, elektron tijorat, shuningdek zamonaviy insonning fikrlash tarziga o‘zining ijobiy ta’siri bilan kirib keldi. Hayot sifatini yaxshilash bilan bog‘liq bo‘lgan ushbu o‘zgarishlar bilan bir qatorda, jinoyatchilikning yangi shakllarini rivojlantirishga qulay sharoitlar paydo bo‘lganligini ta’kidlash lozim. Mazkur jinoyatlar o‘z navbatida “Axborot texnologiyalari sohasidagi jinoyatlar ” (elektron jinoyatlar) deb nomlanadi.

Axborot texnologiyalarining keng miqyosda rivojlanishi bir vaqtning o‘zida ko‘p turdagi jinoyatlarning sodir etilishiga imkon yaratdi, o‘z navbatida ushbu turdagi jinoyatlarni aniqlash va ularni oldini olishda yuqori bilim va kasbiy tayyorgarlikni talab qilmoqda. Shunday qilib, “axborot texnologiyalari sohasidagi jinoyat” kompyuterlar va ma’lumotlarni qayta ishlash tizimlaridan foydalangan holda sodir etiladigan jinoiy qilmish bo‘lib, buning uchun qonunchilikda jinoiy javobgarlik nazarda tutilgan. Shu bois, fuqarolar o‘rtasida axborot texnologiyalari sohasidagi jinoyatlar to‘g‘risida ma’lumotlarni tarqatish va targ‘ibot-tashviqot ishlarini olib borish zarur.

Axborot texnologiyalarining doimiy rivojlanishi va internetning paydo bo‘lishi bilan “Axborot texnologiyalari sohasidagi jinoyatlar” tushunchasi shakllandi. elektron jinoyatlarning asosiy farqi shundaki, ularning ba’zilari kompyuter yordamida (kompyuter jinoyatlari), boshqalari internet (kiberjinoyatlar) orqali sodir etiladi.[1]

Elektron jinoyat shakllari ko‘p qirrali bo‘lib, texnologiyalar va internetning doimiy rivojlanishi bilan tobora ortib bormoqda. Shuningdek, ushbu jinoyatlarni aniqlash va fosh etishda bir qator qiyinchiliklar mavjud bo‘lib, ulardan biri fuqarolarning o‘ziga nisbatan sodir etilgan kompyuter huquqbuzarligi to‘g‘risida huquqni muhofaza qiluvchi

organlarga xabar berishni istamasliklari va kompyuter jinoyatlariga duch kelganda huquqiy bilimlari yetarli emasligi bilan bog‘liqligini taqozo etmoqda .

Axborot texnologiyalari sohasidagi jinoyatlarning ayrim turlarini quyidagilarda ko‘rish mumkin:

- virusli dasturiy ta’minotni tarqatish;
- foydalanuvchining maxfiy ma’lumotlarini o‘g‘irlash;
- boshqa odamlarning intellektual faoliyat mahsulotlarini o‘g‘irlash;
- ijtimoiy tarmoqlarda boshqalarning akkauntlarini buzish;
- yolg‘on ma’lumot tarqatish, tuhmat qilish;
- millatlararo nizo yoki dinlararo adovatni qo‘zg‘atish;
- bank plastik kartalari (karta rekvizitlari) bilan noqonuniy operatsiyalar;
- qimmatli qog‘ozlar bozoridagi internet-firibgarlik;
- Internetdagi moliyaviy piramidalar;
- mobil aloqa bilan bog‘liq jinoyatlar;
- elektron tijorat sohasidagi boshqa jinoyatlar.

Tarmoqda uchraydigan hujumlarni oldini olishda qo‘llash mumkin bo‘lgan ba’zi bir jihatlar quyida keltirib o‘tiladi:

Xavfsizlik devori (Firewall) - kompyuter tarmog‘ining dasturiy yoki dasturiy-apparat elementi bo‘lib, u orqali o‘tadigan tarmoq trafigini belgilangan qoidalarga muvofiq boshqaradi va filtrlaydi.

Xavfsizlik devorlari hal qiladigan vazifalar orasida asosiysi OSI tarmoq modeli protokollari yoki tarmoq kompyuterlarida o‘rnatilgan dasturiy ta’minotdagi zaifliklardan foydalangan holda tarmoq segmentlarini yoki alohida xostlarni ruxsatsiz kirishdan himoya qilishdir. Xavfsizlik devorlari uning xarakteristikalarini avvaldan berilgan qiymatlar bilan solishtirish orqali trafikka ruxsat beradi yoki rad etadi. Xavfsizlik devorlarini o‘rnatishning eng keng tarqalgan joyi ichki xostlarni tashqi hujumlardan himoya qilish uchun mahalliy tarmoq perimetri bo‘ylab joylashadi. Shu bilan birga, hujumlar ichki tugunlardan ham boshlanishi mumkin – bu holda, agar hujum qilingan xost bir tarmoqda joylashgan bo‘lsa, trafik tarmoq perimetrini kesib o‘tmaydi va xavfsizlik devori faollashtirilmaydi.

Shu sababli, hozirgi vaqtda xavfsizlik devori nafaqat chegarada, balki turli xil tarmoq segmentlari o‘rtasida ham joylashtirilgan, bu esa qo‘shimcha xavfsizlik darajasini ta’minlaydi. Xavfsizlik devorlarining yangi avlodi ixcham, yuqori tezlikdagi kirish shlyuziga ega bo‘lib, u tarmoq xavfsizligi va trafikni boshqarish uchun keng qamrovli yechimni, jumladan kuchli, moslashtiriladigan spamga qarshi himoyani, turli tarmoq ob’yektlari uchun tarmoqli kengligi nazoratini, bosqinning oldini olishni va masofadan boshqarishni o‘z ichiga oladi. Virtual xususiy tarmoqlardan foydalangan holda ulanish xavfsizligini ta’minlaydi. Xavfsizlik devori qurilmalari qimmat bo‘lganligi sababli ko‘pgina tashkilotlar sotib olishga mablag‘ muammosi tufayli sotib olmaydilar.

Oqibatda tashkilotning tarmoqdagi platformalari va serverlariga hujumlar uchrab turadi. Qurilma o‘zaro navigatsiya tizimi, o‘rnatilgan qo‘llanma va grafik holat monitoringi bilan intuitiv foydalanuvchi interfeysiga ega. Ob’ektga yo‘naltirilgan boshqaruv modeli hatto murakkab tarmoqlarda ham konfiguratsiyani maksimal darajada optimallashtirish imkonin beradi. LDAP/MS AD/RADIUS-ni qo‘llab-quvvatlash mavjud tarmoqamaliyotlari asosida xavfsizlik siyosatlarini tuzishga yordam beradi.[2]

Trafikni filtrlash qoidalar to‘plami deb ataladigan oldindan tuzilgan qoidalar to‘plamiga asoslanadi. Firewallni axborot oqimini qayta ishlovchi filtrlar qatori deb tasavvur qilish qulay. Filtrlarning har biri alohida qoidani sharhlash uchun mo‘ljallangan. To‘plamdagi qoidalar ketma-ketligi xavfsizlik devorining ishlashiga sezilarli ta’sir qiladi.Misol uchun, ko‘pgina xavfsizlik devorlari mos kelgunga qadar trafikni qoidalar bilan ketma-ket taqqoslaydi. Bunday xavfsizlik devorlari uchun eng ko‘p trafikka mos keladigan qoidalar ro‘yxatda iloji boricha yuqori joylashtirilishi kerak, bu esa unumdorlikni oshiradi.

Kiruvchi trafikni qayta ishlashning ikkita printsipi mavjud. Birinchi tamoyilda aytilishicha: “Aniq ta’qiqlanmagan narsaga ruxsat beriladi”. Bunday holda, agar xavfsizlik devori hech qanday qoidaga to‘g‘ri kelmaydigan paketni olgan bo‘lsa, u keyin uzatiladi. Qarama-qarshi printsip - “Aniq ruxsat etilmagan narsa taqiqlangan” - bu qoidalar bilan aniq ruxsat etilmagan barcha trafikni taqiqlaganligi sababli ancha katta xavfsizlikni kafolatlaydi. Biroq, bu tamoyil administrator uchun qo‘shimcha yuk bo‘lib qoladi.

Oxir-oqibat, xavfsizlik devorlari kiruvchi trafik bo‘yicha ikkita operatsiyadan birini bajaradi: paketni uzatadi (ruxsat beradi) yoki paketni o‘chiradi (rad etadi). Ba’zi xavfsizlik devorlari boshqa operatsiyaga ega - rad etish, bunda paket o‘chiriladi, ammo jo‘natuvchiga u kirishga harakat qilgan xizmat mavjud emasligi haqida xabar beriladi. Bundan farqli o‘laroq, rad etish operatsiyasi jo‘natuvchiga xizmatning mavjud emasligi haqida xabar bermaydi, bu esa xavfsizroqdir.

Boshqariladigan kommutatorlar ba’zan xavfsizlik devori sifatida tasniflanadi, chunki ular tarmoqlar yoki tarmoq tugunlari orasidagi trafikni filtrlaydi. Biroq, ular bog‘lanish darajasida ishlaydi va mahalliy tarmoq ichidagi trafikni ajratadi ya’ni ularni tashqi tarmoqlardan (masalan, Internetdan) trafikni qayta ishlash uchun ishlatib bo‘lmaydi.

Cisco, Nortel, 3Com, ZyXEL kabi ko‘plab tarmoq uskunalari ishlab chiqaruvchilari o‘z kommutatorlarida freym sarlavhalaridagi MAC manzillari asosida trafikni filtrlash imkoniyatini taqdim etadilar. Masalan, Cisco Catalyst oilasining kommutatorlarida bu funksiya Port Security mexanizmi yordamida amalga oshiriladi. Biroq, ushbu filtrlash usuli samarali emas, chunki tarmoq kartasining apparatida o‘rnatilgan MAC manzili dasturiy ta’minot orqali osongina o‘zgartirilishi mumkin, chunki drayver orqali ko‘rsatilgan qiymat plataga ulanganidan ko‘ra yuqoriroq

ustuvorlikka ega. Shuning uchun ko‘plab zamonaviy kommutatorlar filtrlash belgisi sifatida boshqa parametrlardan foydalanishga imkon beradi - masalan, VLAN ID. Virtual mahalliy tarmoq texnologiyasi boshqa tarmoq tugunlaridan trafigini to‘liq izolyatsiya qilgan xostlar guruhlarini yaratish imkonini beradi.[3]

Boshqariladigan kommutatorlarga asoslangan korporativ tarmoq ichida xavfsizlik siyosatini amalga oshirish kuchli va juda arzon yechim bo‘lishi mumkin. Faqat havola-qatlam protokollari bilan o‘zaro aloqada bo‘lgan ushbu xavfsizlik devorlari trafikni juda yuqori tezlikda filtrlaydi.

Ushbu yechimning asosiy kamchiligi yuqori darajadagi protokollarni tahlil qilishning mumkin emasligidadir. Xavfsizlik devori samarali o‘rnatilgan tashkilotlarda joylashgan xosting vazifasini bajaruvchi serverlarning ishonchliligi ortadi. Tashqaridan ushbu serverga qilinadigan murojat tez, qulay va xavfsiz bo‘ladi.

Xulosa qilib aytganda, tashkilotlarning tarmoqlari xavfsiz va sifatli ishlashida xavfsizlik devori alohida o‘rniga ega hisoblanadi. Tarmoq tashkil qilishda apparat vositalarini to‘g‘ri sozlash, boshqarish va doimiy nazorat qilish AKT joriy etilishining mukammalligiga erishishga imkoniyat beradi. Firewall qurilmalarini yurutishda malakali tarmoq administratorlariga extiyoj tobora ortib bormoqda. Yuqoridagilardan kelib chiqadiki, zamonaviy tarmoq qurilmalari va malakali mutaxassislar eng katta o‘rin tutadi.

FOYDALANILGAN ADABIYOTLAR:

1. G‘ulomov Sherzod Rajaboyevich, Odilov Ilhom Isoq o‘g‘li, Bozorova Feruza Xaydar qizi, Tashkilotlarda tarmoq xavfsizligini himoyalashning ayrim jihatlari Kibermakonda sodir etilayotgan jinoyatlarga qarshi kurash: muammolar va yechimlar: Respublika ilmiy-amaliy konferensiya materiallari to‘plami. 2022-yil
2. Баранова, Е.К. Методики анализа и оценки рисков информационной безопасности / Е.К. Баранова // Образовательные ресурсы и технологии. – 2015
3. Аникин, И.В. Обеспечение информационной безопасности корпоративных информационных сетей через оценку и управление рисками / И.В. Аникин, Л.Ю. Емалетдинова, А.П. Кирпичников // Вестник технологического университета. – 2015. – Том 18, № 7
4. Ахмедов, Б. А. (2021). Таълимда ахборот технологиялари фанининг модулларини ўқитишда кластерли-инновацион технологиялардан фойдаланиш тамойиллари. O‘zbekiston respublikasi oliy va o‘rta maxsus ta’lim vazirligi, 441.
5. Akhmedov, B. A. (2023). Improvement of the digital economy and its significance in higher education in tashkent region. Uzbek Scholar Journal, 12, 18-21.
6. Akhmedov, B. A. (2023). Innovative pedagogical technologies in the modern educational system. World Bulletin of Social Sciences, 19, 107-112.

7. Akhmedov, B. A. (2022). Use of Information Technologies in The Development of Writing and Speech Skills. Uzbek Scholar Journal, 9, 153-159.
8. Akhmedov, B. A. (2022). Psychological and pedagogical possibilities of forming tolerance in future teachers. Uzbek Scholar Journal, 11, 289-295.
9. Akhmedov, B. A. (2023). Methods to increase algorithmic thinking in primary education. Uzbek Scholar Journal, 12, 22-26.
10. Ахмедов, Б. А. (2023). Интегралашган таълимда талабалар билимларини виртуал тест назорат қилиш тизимларини ишлаб чиқиш концепцияси. PEDAGOG, 1(5), 86-92.
11. Akhmedov, B. A. (2022). Principles of Developing the Professional Competence of Future Teachers on the basis of a Cluster Approach. Galaxy International Interdisciplinary Research Journal, 10(6), 760-770.