KICHIK KORXONA UCHUN LOKAL TARMOQNI LOYIHALASH VA AXBOROT XAVFSIZLIGINI TA’MINLASHNING AMALIY YECHIMLARI

Umarova Gulshan Kaxorovna

Umarova Madina Shaxobiddin qizi

Zarafshon shahar 2-son texnikumi Maxsus fan o’qituvchilari

PRACTICAL SOLUTIONS FOR DESIGNING A LOCAL NETWORK AND ENSURING INFORMATION SECURITY FOR A SMALL ENTERPRISE

Umarova Gulshan Kahorovna

Umarova Madina Shakhobiddin kizi

Teachers of special subjects, Zarafshan city technical school No. 2

Annotatsiya. Ushbu maqolada kichik korxona sharoitida lokal tarmoqni amaliy loyihalash va axborot xavfsizligini tizimli ta’minlash masalalari yoritiladi. Asosiy e’tibor tarmoqni biznes ehtiyojlariga mos rejalash, segmentatsiya orqali xavflarni kamaytirish, ishonchli ulanish va xizmatlarni barqaror ishlatish hamda boshqaruv, nazorat, zaxiralash kabi xavfsizlik mexanizmlarini joriy etishga qaratiladi. Adabiyotlar sharhida tarmoq arxitekturasi bo‘yicha klassik yondashuvlar, tarmoq xavfsizligi tamoyillari, kichik biznes uchun riskka asoslangan boshqaruv, amaliy nazoratlar majmui hamda axborot xavfsizligi boshqaruv tizimi talablarining o‘zaro bog‘liqligi tahlil qilinadi.

Kalit so‘zlar: lokosin tarmoq, kichik korxona, tarmoq loyihalash, VLAN segmentatsiya, Wi-Fi xavfsizligi, firewall, kirishni boshqarish, zaxiralash, monitoring, riskni boshqarish.

Аннотация. В статье рассматриваются практические решения по проектированию локальной сети для малого предприятия и обеспечению информационной безопасности на основе системного подхода. Основной акцент сделан на согласовании сетевой архитектуры с бизнес задачами, снижении рисков за счет сегментации, обеспечении надежной связности и сервисов, а также внедрении управленческих и технических мер безопасности.

Ключевые слова: локальная сеть, малое предприятие, проектирование сети, сегментация VLAN, безопасность Wi-Fi, межсетевой экран, управление доступом, резервное копирование, мониторинг, управление рисками

Abstract. This article discusses practical solutions for designing a small business local area network and ensuring information security through a structured approach. The focus is on aligning network architecture with business needs, reducing risks via segmentation, ensuring reliable connectivity and services, and implementing both governance and technical security controls.

Keywords: small business network, LAN design, VLAN segmentation, wireless security, firewall, access management, backup, logging, monitoring, risk management.

KIRISH

Kichik korxonada lokal tarmoq ko‘pincha biznesning yuragi bo‘lib qoladi: hisob va savdo tizimlari, hujjatlar aylanishi, pochta, mijozlar bazasi, kassalar, printerlar, videokuzatuv, bulut xizmatlari va masofadan ishlash aynan tarmoq orqali yashaydi. Shunga qaramay, amaliyotda tarmoq ko‘pincha shoshilinch ehtiyoj bilan yig‘iladi: bir nechta yo‘riqnoma, arzon kommutator, paroli hammaga ma’lum Wi-Fi va tayinlanmagan mas’uliyat. Bunday holat birinchi oylar ishlayotgandek ko‘rinadi, keyin esa uzilishlar, tezlik muammosi, ichki resurslarga ruxsatsiz kirish, ma’lumot yo‘qolishi, virus va fishingdan zarar, audit va tekshiruvlarda tushunmovchiliklar paydo bo‘ladi. Tarmoqni to‘g‘ri loyihalash esa faqat sim ulash emas, u biznes

jarayonlarini tushunish, tarmoq qatlamlari bo‘yicha aniq arxitektura tuzish, kirishni boshqarish, xavfsizlik siyosatlarini belgilash, zaxira va monitoringni yo‘lga qo‘yish degani.

Zamonaviy yondashuv tarmoq xavfsizligini alohida texnik vazifa sifatida emas, boshqariladigan risklar majmui sifatida ko‘radi. Bunda korxona o‘z aktivlarini aniqlaydi, tahdid va zaifliklarni baholaydi, ustuvor himoya choralarini tanlaydi va doimiy takomillashtiradi. NIST kiberxavfsizlik doirasi boshqaruv, aniqlash, himoya, aniqlash, javob, tiklash natijalarini bir tizimga jamlab, kichik tashkilotlarga ham moslashuvchan yo‘l xaritasi beradi [3].

ADABIYOTLAR SHARHI

Lokal tarmoqni loyihalash masalasi avvalo tarmoqning ichki ishlash tamoyillariga borib taqaladi. Tarmoq qatlamlari, uzatish muhiti, marshrutlash va kommutatsiya, kechikish va yuklama, ishonchlilik va xizmat sifati kabi tushunchalar tarmoq arxitekturasini ongli qurish uchun asos bo‘ladi [1]. Klassik yondashuv shuni ko‘rsatadiki, tarmoqdagi muammolarning katta qismi fizik darajada emas, noto‘g‘ri segmentatsiya, adreslash va boshqaruv qarorlaridan kelib chiqadi. Demak, kichik korxona ham tarmoqni shunchaki ulab qo‘yish emas, rejalashga tayanib qurishi kerak.

Tarmoq xavfsizligi bo‘yicha fundamental manbalarda himoya modeli odatda bir nechta qatlamga bo‘linadi: perimetr nazorati, ichki segmentlar, host darajasi, ilova darajasi va boshqaruv darajasi [2]. Bu yondashuv kichik korxona sharoitida ham muhim, chunki faqat bitta firewall yoki faqat antivirus bilan cheklanib bo‘lmaydi. Xavfsizlikning amaliy qiymati shundaki, hujumchi bitta eshikdan kirmasa, u darhol ma’lumotgacha yetib bormaydi, yo‘llar torayadi, izlar qoladi va javob berish osonlashadi.

Riskka asoslangan boshqaruv bo‘yicha NIST doirasi tashkilotning maqsadlarini hisobga olgan holda natijaviy ko‘rsatkichlar orqali xavfsizlikni yo‘lga qo‘yishni tavsiya qiladi va aynan kichik tashkilotlar uchun ham mos keladigan moslashuvchan struktura beradi [3]. Shu bilan uyg‘un ravishda NIST kichik biznes qo‘llanmasi

minimal siyosatlar, aktivlarni ro‘yxatga olish, zaxira, yangilash, ruxsatlar, tashqi xizmatlar va xodimlar xabardorligi kabi amaliy qadamlarni ustuvor deb ko‘rsatadi [4]. Bu ikki manba kichik korxona uchun texnik qarorlar bilan birga tashkiliy choralarni ham bir paketga aylantirish kerakligini isbotlaydi.

TADQIQOT METODOLOGIYASI VA EMPIRIK TAHLIL

Kichik korxona uchun tarmoq loyihasi odatda uch savoldan boshlanadi: kim ishlaydi, nima ishlaydi, qachon ishlaydi. Kim deganda foydalanuvchilar va qurilmalar nazarda tutiladi: xodim kompyuteri, noutbuk, telefon, printer, kamera, ombor skaneri, kassalar, server yoki NAS, mehmon qurilmalari. Nima deganda xizmatlar nazarda tutiladi: internet, ichki fayl almashish, buxgalteriya tizimi, CRM, videokuzatuv, IP telefon, bulut ilovalari, masofadan ulanish. Qachon deganda ish rejimi, yuklama cho‘qqilari, uzilishning biznesga ta’siri va xizmat ko‘rsatish vaqtlarining imkoniyati nazarda tutiladi. NIST kichik biznes tavsiyalarida aktivlarni aniqlash va riskni tushunish birinchi qadam sifatida keltirilishi bejiz emas [4]. Aynan shu bosqichda xavfsizlik talablari ham chiziladi: kimga qaysi resurs kerak, nimalar umumiy, nimalar ajratilgan bo‘lishi shart, qaysi ma’lumot eng qimmat, qaysi xizmat to‘xtasa biznes to‘xtaydi.

NATIJALAR

Kichik ofis uchun eng barqaror topologiya markazlashgan yulduz prinsipiga tayanadi: barcha ish joylari markaziy kommutatorga keladi, u yerda marshrutlash va xavfsizlik perimetr qurilmasi bilan bog‘lanadi. Bu yondashuv tarmoqni boshqarishni osonlashtiradi, nosozlikni tez topishga yordam beradi va kengayishga qulay [1]. Kabellashda keyingi yillarda talab oshishini hisobga olib, ish joyiga kamida ikki port rejalash amaliy jihatdan to‘g‘ri, chunki bir port kompyuterga, ikkinchisi IP telefon, printer yoki qo‘shimcha qurilmaga ketishi mumkin. Wi-Fi esa kabelning o‘rnini to‘liq bosmaydi, u mobil ish uslubi va mehmonlar uchun qulay qatlam bo‘lib xizmat qiladi. Wi-Fi ni boshqariladigan nuqtalar orqali, qamrov zonasi va kanal rejasini hisobga olib

qurish uzilishlarni kamaytiradi, ayniqsa ko‘p kvartirali binolarda interferensiya muammo bo‘lishi mumkin.

Uzluksizlik uchun kichik korxonada ham minimal energiya himoyasi zarur: markaziy tarmoq tugunlari uchun uzluksiz quvvat manbai, to‘g‘ri yerga ulash, ortiqcha kuchlanishdan himoya. Bu xavfsizlikning bir qismi, chunki elektr muammolari ko‘pincha konfiguratsiya buzilishiga, ma’lumot yo‘qolishiga va tiklash vaqtining cho‘zilishiga olib keladi. ISO talablari doirasida uzluksizlik va resurslarni ta’minlash boshqaruvning ajralmas bo‘lagi sifatida qaraladi [6].

Kichik korxona tarmog‘ining eng katta amaliy yutug‘i segmentatsiya orqali keladi. Segmentatsiya deganda tarmoqni mantiqiy zonalarga bo‘lish tushuniladi: xodimlar zonasi, server yoki umumiy resurslar zonasi, videokuzatuv zonasi, mehmon Wi-Fi zonasi, boshqaruv zonasi. Buni VLAN asosida amalga oshirish odatda eng qulay yo‘l, chunki bir xil kabel infratuzilmasi ustida alohida mantiqiy tarmoqlar yaratiladi va ular orasidagi trafik nazorat qilinadi [1]. Segmentatsiya sababli bir zonada muammo chiqsa, u darhol hamma joyga tarqalmaydi. Masalan, mehmon Wi-Fi dan faqat internetga chiqishga ruxsat beriladi, ichki fayl server yoki printerlarga yo‘l yopiladi. Videokameralar zonasi esa faqat yozuv qurilmasi yoki monitoring serveri bilan gaplashadi, xodim kompyuterlariga bevosita ko‘rish huquqi cheklanadi. Bu qatlamli himoyaga mos keladi va tarmoq xavfsizligi bo‘yicha tavsiyalarda ichki tarmoqlarni ajratish amaliyoti doimiy urg‘u bilan keltiriladi [2].

Adreslash rejasini boshidan to‘g‘ri tuzish keyinchalik tarmoqni boshqarishni yengillashtiradi. Har bir VLAN uchun alohida subnet ajratish, statik beriladigan qurilmalar ro‘yxatini yuritish, DHCP orqali dinamik manzillarni nazorat qilish, DNS ni tartibli ishlatish kichik tarmoqda ham intizom beradi. CIS Controls doirasida aktivlar hisobini yuritish va xavfsiz konfiguratsiya ustuvor vazifa bo‘lgani uchun adreslash va konfiguratsiya hujjati oddiy ko‘rinishda bo‘lsa ham, muntazam yangilanib borishi kerak [5]. Natijada hodisa yuz bersa, kim qayerda ulanganini, qaysi qurilma qaysi zonada ekanini tez aniqlash mumkin bo‘ladi.

Kichik korxona uchun eng ko‘p xato qilinadigan joy internet perimetri. Birinchi qoida shunday: ichki tarmoqqa bevosita kirish portlarini internetga ochib qo‘yish kerak emas. Masofaviy ish zarur bo‘lsa, VPN orqali, kuchli autentifikatsiya bilan va ruxsatlar minimal prinsipi bo‘yicha yo‘lga qo‘yiladi [2]. NIST doirasidagi himoya natijalari va NIST kichik biznes tavsiyalarida ham masofaviy kirish, hisoblar, yangilash, zaxira kabi bazaviy yo‘nalishlar ustuvor hisoblanadi [3], [4]. Amaliy jihatdan VPN foydalanuvchisi ham segmentatsiya qoidalariga bo‘ysunishi kerak: u hamma narsaga emas, o‘z ishiga kerak resurslargagina kiradi.

XULOSA VA MUNOZARA

Kichik korxona uchun lokal tarmoqni loyihalash va axborot xavfsizligini ta’minlashning eng to‘g‘ri yo‘li texnik va tashkiliy choralarni bir butun ko‘rishdan boshlanadi. Tarmoq arxitekturasi qatlamlar mantiqiga tayanib qurilganda, segmentatsiya orqali ichki risklar boshqarilganda, perimetr va masofaviy kirish tartibli yo‘lga qo‘yilganda, loglar va zaxira tizimi ishlaganda, korxona nafaqat tez ishlaydigan, balki tiklanadigan infratuzilmaga ega bo‘ladi. Adabiyotlar shuni ko‘rsatadiki, tarmoqning barqaror ishlashi uchun rejalash va qatlamli arxitektura muhim, xavfsizlik uchun esa ko‘p qatlamli himoya, minimal ruxsat va nazorat mexanizmlari zarur. Riskka asoslangan boshqaruv yondashuvi kichik korxonaga xavfsizlikni bosqichma bosqich yo‘lga qo‘yish imkonini beradi, kichik biznes bo‘yicha amaliy tavsiyalar esa ortiqcha murakkabliksiz minimal paketni beradi.

ADABIYOTLAR RO`YXATI

1. Tanenbaum A. S., Feamster N., Wetherall D. J. Computer Networks. 6th edition. Harlow: Pearson, 2021. 960 p.
2. Stallings W. Network Security Essentials: Applications and Standards. 6th edition. Boston: Pearson, 2021. 480 p.
3. National Institute of Standards and Technology. The NIST Cybersecurity Framework CSF 2.0. NIST CSWP 29. Gaithersburg: NIST, 2024.

4. Paulsen C., Toth P. Small Business Information Security: The Fundamentals. NISTIR 7621 Revision 1. Gaithersburg: NIST, 2016.
5. Center for Internet Security. CIS Critical Security Controls Version 8.1. East Greenbush: CIS, 2024.
6. ISO, IEC. ISO IEC 27001:2022 Information security management systems Requirements. Geneva: ISO, 2022.