LOKAL VA GLOBAL KOMPYUTER TARMOQLARINI TASHKIL ETISH, BOSHQARISH HAMDA TARMOQ XAVFSIZLIGINI TA’MINLASHNING ZAMONAVIY YECHIMLARI

RUZIQULOVA MUXAYYO RUZIQULOVNA
Navoiy viloyati Uchquduq tuman
1-son texnikumi maxsus fan o‘qituvchisi
Kompyuter tarmoqlari va adminstratorlash fani

ANNOTATSIYA

Mazkur maqolada lokal (LAN) va global (WAN) kompyuter tarmoqlarini tashkil etish, boshqarish hamda tarmoq xavfsizligini ta’minlashning zamonaviy texnologiyalari va yechimlari ilmiy jihatdan tahlil qilingan. Tarmoq infratuzilmasini loyihalash tamoyillari, TCP/IP modeli, OSI modeli, marshrutlash (routing), kommutatsiya (switching), VLAN, VPN, SD-WAN, IPv6, simli va simsiz tarmoqlarni boshqarish usullari hamda zamonaviy tarmoq arxitekturalari yoritilgan. Shuningdek, tarmoq xavfsizligini ta’minlashda qo‘llaniladigan autentifikatsiya, avtorizatsiya, shifrlash algoritmlari, xavfsizlik devorlari (Firewall), hujumlarni aniqlash va oldini olish tizimlari (IDS/IPS), Zero Trust Architecture, ko‘p faktorli autentifikatsiya (MFA), virtual xususiy tarmoqlar (VPN) va tarmoq monitoringi vositalarining amaliy ahamiyati tahlil qilingan.

Kalit so‘zlar: lokal tarmoq (LAN), global tarmoq (WAN), kompyuter tarmoqlari, OSI modeli, TCP/IP protokoli, marshrutlash (Routing), kommutatsiya (Switching), VLAN, VPN, SD-WAN, IPv6.

KIRISH

Tarmoq arxitekturasini tashkil etishda OSI va TCP/IP modellariga asoslangan ko‘p pog‘onali yondashuv asosiy metodologiya hisoblanadi. Zamonaviy LAN infratuzilmasida yuqori tezlikdagi Ethernet, Layer-2 va Layer-3 kommutatsiyasi, VLAN segmentatsiyasi, dinamik marshrutlash protokollari (OSPF, BGP, IS-IS), IPv6 adreslash tizimi va virtualizatsiyalash texnologiyalari keng qo‘llanilmoqda. WAN infratuzilmasida esa

MPLS, VPN, SD-WAN va Cloud Networking yechimlari tarmoqlarni markazlashgan boshqarish imkoniyatini yaratmoqda.

2020-yil 11-avgustda AQShning National Institute of Standards and Technology (NIST) tomonidan Special Publication 800-207 – Zero Trust Architecture e'lon qilindi. Ushbu hujjatda zamonaviy tarmoq xavfsizligining asosiy tamoyili sifatida "Never Trust, Always Verify" konsepsiyasi tavsiya etildi. Mazkur modelga ko'ra foydalanuvchi, qurilma yoki xizmat lokal tarmoq ichida joylashgan bo'lsa ham avtomatik ravishda ishonchli deb qabul qilinmaydi. Har bir ulanish identifikatsiya, autentifikatsiya, avtorizatsiya va xavf darajasi bo'yicha real vaqt rejimida tekshiriladi. NIST ekspertlari ushbu yondashuvni masofaviy ishchi stansiyalar, BYOD qurilmalari, bulutli platformalar va gibrid tarmoqlar xavfsizligini ta'minlashning eng samarali usullaridan biri sifatida tavsiya qilgan.

ASOSIY QISM

Zero Trust Architecture konsepsiyasida asosiy e'tibor tarmoq perimetrini emas, balki resurslarni himoyalashga qaratiladi. Har bir foydalanuvchi sessiyasi boshlanishidan oldin ko'p faktorli autentifikatsiya (MFA), qurilma holatini tekshirish (Device Validation), identifikatsiyani boshqarish (IAM), mikrosegmentatsiya (Micro-Segmentation), minimal huquqlar tamoyili (Least Privilege Access) hamda uzluksiz monitoring mexanizmlari qo'llaniladi. Bunday arxitektura ichki va tashqi kiberhujumlar natijasida yuzaga keladigan lateral harakatlarni sezilarli darajada cheklaydi.

Korporativ WAN infratuzilmasida oxirgi yillarda Software-Defined Wide Area Network (SD-WAN) texnologiyasi keng joriy etilmoqda. SD-WAN tarmoqni dasturiy boshqarish orqali trafikni avtomatik optimallashtirish, ilovalar ustuvorligini belgilash, markazlashgan konfiguratsiya va real vaqt monitoringini ta'minlaydi. Ushbu texnologiya MPLS, Internet va LTE/5G kanallarini yagona boshqaruv platformasida birlashtirish imkonini beradi. Natijada tarmoqning uzluksizligi, o'tkazuvchanligi va ishonchliligi sezilarli darajada oshadi.

Zamonaviy tarmoq xavfsizligining muhim komponentlaridan biri Network Access Control (NAC) tizimidir. Ushbu tizim foydalanuvchilar va qurilmalarni tarmoqqa ulanishidan oldin identifikatsiyalaydi, xavfsizlik siyosatlariga mosligini tekshiradi va faqat

talablarni qanoatlantirgan qurilmalarga kirish huquqini beradi. NAC yechimlari Endpoint Detection and Response (EDR), Identity and Access Management (IAM) hamda Security Information and Event Management (SIEM) platformalari bilan integratsiyalashgan holda ishlaydi.

Mazkur tahlilda klassik tarmoq xavfsizligi modeli endilikda zamonaviy kiberxavflarga to‘liq javob bera olmasligi ko‘rsatildi. Bulutli hisoblash (Cloud Computing), Internet of Things (IoT), 5G infratuzilmalari, masofaviy ishlash (Remote Work) va gibrid tarmoqlarning keng joriy etilishi natijasida korporativ tarmoqlarda hujum yuzasi (Attack Surface) sezilarli darajada kengaygan. Hisobotda ayniqsa identifikatsiyani boshqarish, tarmoq segmentatsiyasi, real vaqt monitoringi, zaifliklarni boshqarish (Vulnerability Management) va uzluksiz xavf tahlili zamonaviy tarmoq boshqaruvining asosiy komponentlari sifatida belgilangan.

Hisobotda zamonaviy LAN va WAN infratuzilmalarini boshqarishda riskga asoslangan boshqaruv modeli (Risk-Based Network Management) tavsiya etiladi. Ushbu modelga ko‘ra tarmoq administratorlari avvalo barcha apparat va dasturiy resurslarni inventarizatsiya qiladi, ularning kritiklik darajasini baholaydi, so‘ng xavf ehtimoli va ta'sir ko‘rsatkichlari asosida himoya choralarini ustuvorlashtiradi. Bunday yondashuv resurslardan samarali foydalanish hamda kiberhujumlarning oldini olish imkonini beradi.

Tahlilda Zero Trust Network Architecture, Network Access Control (NAC) va Identity and Access Management (IAM) texnologiyalari korporativ tarmoqlarning asosiy himoya mexanizmlari sifatida tavsiya etilgan. Mazkur texnologiyalar yordamida foydalanuvchi, qurilma va xizmatlarning har bir ulanishi alohida tekshiriladi, ko‘p faktorli autentifikatsiya (MFA), minimal huquqlar tamoyili (Least Privilege) hamda doimiy sessiya nazorati qo‘llaniladi. Natijada ichki foydalanuvchilar tomonidan yuzaga keladigan tahdidlar va lateral harakatlar sezilarli darajada kamayadi.

XULOSA

2024-yil 17-oktabrda European Commission NIS2 direktivasining texnik amalga oshirish reglamentini ham qabul qildi. Unda DNS provayderlari, ma'lumotlar markazlari (Data Centers), bulutli xizmat ko‘rsatuvchilar, boshqariladigan xizmat provayderlari

(MSP), boshqariladigan xavfsizlik xizmatlari (MSSP) hamda kontent yetkazib berish tarmoqlari (CDN) uchun kiberxavfsizlik risklarini boshqarish bo‘yicha minimal texnik talablar belgilab berildi. Mazkur hujjat tarmoq segmentatsiyasi, zaxiralash, hodisalarni qayd etish (Logging), uzluksiz monitoring va favqulodda tiklash (Disaster Recovery) mexanizmlarini majburiy element sifatida belgilaydi.

Mazkur xalqaro tajriba shuni ko‘rsatadiki, zamonaviy lokal va global kompyuter tarmoqlarini samarali boshqarish faqat yuqori tezlikdagi apparat vositalariga emas, balki xavfga asoslangan boshqaruv siyosati, Zero Trust tamoyillari, avtomatlashtirilgan monitoring, sun'iy intellekt asosidagi tahdidlarni aniqlash, tarmoq segmentatsiyasi va uzluksiz audit mexanizmlarining kompleks qo‘llanilishiga bog‘liq. Aynan shu yondashuvlar korporativ infratuzilmalarning barqarorligini oshirish, kiberhujumlarga bardoshliligini kuchaytirish va axborot resurslarining maxfiyligi, yaxlitligi hamda mavjudligini ta'minlashning eng samarali yechimlari sifatida e'tirof etilmoqda.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. National Institute of Standards and Technology (NIST). *Special Publication 800-207: Zero Trust Architecture*. Gaithersburg, MD: NIST, 2020.
2. European Union Agency for Cybersecurity (ENISA). *2024 Report on the State of Cybersecurity in the Union*. Athens: ENISA, 2024.
3. European Union Agency for Cybersecurity (ENISA). *ENISA Threat Landscape 2024*. Athens: ENISA, 2024.
4. Internet Engineering Task Force (IETF). *RFC 8200: Internet Protocol, Version 6 (IPv6) Specification*. Fremont, CA: RFC Editor, 2017.