KOMPYUTER TARMOQLARINI ADMINISTRATSIYALASHDA AXBOROT XAVFSIZLIGINI TA'MINLASHNING ZAMONAVIY USULLARI

Meliboyeva Nilufar Abduvositovna
Farg'ona viloyati Rishton tumani 1-son texnikumi Kompyuter tarmoqlarini adminstratsiyalash fani o'qituvchisi

Annotatsiya. Mazkur maqolada kompyuter tarmoqlarini administratsiyalash jarayonida axborot xavfsizligini ta'minlashning zamonaviy usullari ilmiy-amaliy jihatdan tahlil qilingan. Tarmoq administratsiyasining asosiy vazifalari, axborot xavfsizligining fundamental tamoyillari, zamonaviy kiberxavflar hamda ularga qarshi qo'llaniladigan himoya vositalari yoritilgan. Shuningdek, xavfsizlik devorlari (Firewall), virtual xususiy tarmoqlar (VPN), tarmoq segmentatsiyasi, IDS/IPS tizimlari, SIEM platformalari, zaxira nusxalarini yaratish, tarmoq monitoringi va avtomatlashtirish texnologiyalarining kompyuter tarmoqlari xavfsizligini ta'minlashdagi o'rni tahlil qilingan.

Kalit so'zlar: tarmoq, administratsiya, kiberxavfsizlik, Firewall, VPN, VLAN, autentifikatsiya, monitoring, shifrlash, segmentatsiya, zaxiralash.

KIRISH

Bugungi kunda axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida kompyuter tarmoqlari davlat boshqaruvi, ta'lim, sanoat, bank-moliya va boshqa ko'plab sohalarning muhim infratuzilmasiga aylandi. Tarmoqlar orqali katta hajmdagi ma'lumotlar uzatilishi va saqlanishi axborot xavfsizligini ta'minlash masalasini dolzarb vazifalardan biriga aylantirmoqda. Turli xil kiberhujumlar, ruxsatsiz kirishlar va zararli dasturlar tarmoq resurslarining ishonchli himoyalanishini talab etadi. Kompyuter tarmoqlarini administratsiyalash jarayonida tarmoqning uzluksiz ishlashini ta'minlash bilan bir qatorda foydalanuvchilarni boshqarish, ma'lumotlarni himoyalash, tarmoq qurilmalarini nazorat qilish hamda xavfsizlik siyosatini amalga oshirish muhim ahamiyat kasb etadi. Shu sababli zamonaviy administratsiyada Firewall, VPN, tarmoq monitoringi, autentifikatsiya, segmentatsiya va boshqa xavfsizlik texnologiyalaridan kompleks foydalanish zarur hisoblanadi.

ASOSIY QISM

Kompyuter tarmoqlarining rivojlanishi bilan axborot resurslarining qiymati va ulardan foydalanish ko'lami keskin kengaydi. Korxona, tashkilot va ta'lim muassasalarining deyarli barcha faoliyati tarmoq infratuzilmasi orqali amalga oshirilayotganligi sababli axborot xavfsizligini ta'minlash masalasi kompyuter tarmoqlarini administratsiyalashning ajralmas qismiga aylandi. Zamonaviy tarmoq administratori nafaqat tarmoq qurilmalarini sozlash va texnik xizmat ko'rsatish bilan shug'ullanadi, balki axborotning maxfiyligi, yaxlitligi va mavjudligini kafolatlovchi xavfsizlik mexanizmlarini ishlab chiqish hamda amaliyotga joriy etish uchun ham

mas’ul hisoblanadi. Shu sababli bugungi kunda tarmoq administratoridan operatsion tizimlar, server texnologiyalari, marshrutlash protokollari va kommutatsiya usullari bilan bir qatorda zamonaviy kiberxavfsizlik vositalari bo‘yicha ham chuqur bilim talab etiladi.

Axborot xavfsizligi uchta asosiy tamoyil – maxfiylik (Confidentiality), yaxlitlik (Integrity) va mavjudlik (Availability) tamoyillariga asoslanadi. Mazkur tamoyillar xalqaro amaliyotda CIA modeli deb yuritiladi. Maxfiylik tamoyili ma’lumotlardan faqat tegishli vakolatga ega foydalanuvchilarning foydalanishini ta’minlashni nazarda tutadi. Bunda foydalanuvchilarni identifikatsiyalash, autentifikatsiya qilish va ularning huquqlarini boshqarish muhim o‘rin egallaydi. Yaxlitlik tamoyili axborotning ruxsatsiz o‘zgartirilmasligini, buzilmasligini yoki yo‘q qilinmasligini kafolatlaydi. Ushbu tamoyil elektron raqamli imzo, nazorat yig‘indilari (Checksum), xesh-funksiyalar hamda ma’lumotlarni zaxiralash texnologiyalari orqali amalga oshiriladi. Mavjudlik tamoyili esa foydalanuvchilarning zarur vaqtda tarmoq resurslari hamda axborot tizimlaridan uzluksiz foydalanish imkoniyatini anglatadi. Mazkur tamoyil serverlarning barqaror ishlashi, zaxira elektr ta’minoti, klasterlash, yuklamani taqsimlash (Load Balancing) hamda avariyadan tiklash tizimlari orqali ta’minlanadi.

Kompyuter tarmoqlarini administratsiyalashda xavfsizlikni tashkil etish bir martalik jarayon emas, balki doimiy ravishda takomillashtirib boriladigan kompleks boshqaruv tizimi hisoblanadi. Har qanday tashkilotning tarmoq infratuzilmasi vaqt o‘tishi bilan yangi qurilmalar, yangi dasturiy vositalar va qo‘shimcha xizmatlar bilan boyib boradi. Natijada yangi zaifliklar va ehtimoliy xavf manbalari ham yuzaga keladi. Administrator ushbu o‘zgarishlarni muntazam tahlil qilib borishi, xavfsizlik siyosatini yangilashi, foydalanuvchilar faoliyatini nazorat qilishi hamda tarmoq konfiguratsiyasini zamonaviy talablar asosida optimallashtirib borishi zarur. Ayniqsa, tashkilotlarda masofadan ishlash texnologiyalarining ommalashuvi, mobil qurilmalar sonining ortishi va bulutli platformalardan foydalanish xavfsizlikni boshqarish jarayonini yanada murakkablashtirmoqda.

Bugungi kunda axborot xavfsizligiga tahdid soluvchi omillar soni va murakkabligi yil sayin ortib bormoqda. Avvallari oddiy virus yoki zararli dasturlar asosiy xavf hisoblangan bo‘lsa, hozirgi davrda murakkab APT (Advanced Persistent Threat) hujumlari, ransomware dasturlari, fishing, spear-phishing, botnet tarmoqlari, DDoS hujumlari, nol kunlik (Zero-Day) zaifliklardan foydalanish hamda ijtimoiy muhandislik usullari keng qo‘llanilmoqda. Ushbu tahdidlarning aksariyati foydalanuvchining ehtiyotsizligi yoki administrator tomonidan xavfsizlik siyosatiga yetarlicha amal qilinmaganligi sababli muvaffaqiyatli amalga oshiriladi. Shu bois texnik himoya vositalari bilan bir qatorda xodimlarning axborot xavfsizligi bo‘yicha bilim va ko‘nikmalarini muntazam oshirib borish ham samarali himoyaning muhim omili hisoblanadi.

Kompyuter tarmoqlarida yuzaga keladigan tahdidlar tashqi va ichki tahdidlarga ajratiladi. Tashqi tahdidlar internet orqali amalga oshiriladigan noqonuniy kirishlar, zararli dasturlar, xakerlik hujumlari hamda xizmat ko‘rsatishni rad etish (DDoS) hujumlari ko‘rinishida namoyon bo‘ladi. Ichki tahdidlar esa tashkilot xodimlarining ehtiyotsizligi, noto‘g‘ri konfiguratsiya, zaif parollar, xizmat vakolatlaridan noto‘g‘ri foydalanish yoki qasddan amalga oshiriladigan noqonuniy harakatlar natijasida yuzaga keladi. Statistik ma’lumotlar shuni ko‘rsatadiki, ko‘plab axborot xavfsizligi hodisalari aynan ichki omillar bilan bog‘liq bo‘ladi. Shuning uchun administrator nafaqat tashqi tarmoq chegaralarini himoyalashi, balki ichki segmentlar, foydalanuvchilar faoliyati va xizmatlarning ishlash holatini ham doimiy monitoring qilib borishi zarur.

Tarmoq administratsiyasida xavfsizlikni ta’minlash ko‘p bosqichli himoya (Defense in Depth) konsepsiyasiga asoslanadi. Ushbu yondashuvga ko‘ra, xavfsizlik faqat bitta vosita yordamida emas, balki bir-birini to‘ldiruvchi bir nechta himoya qatlamlari orqali amalga oshiriladi. Bunday qatlamlarga fizik xavfsizlik, tarmoq perimetrini himoyalash, xavfsizlik devorlari (Firewall), antivirus tizimlari, autentifikatsiya vositalari, foydalanuvchi huquqlarini boshqarish, ma’lumotlarni shifrlash, VPN texnologiyalari, IDS/IPS tizimlari, SIEM platformalari, zaxira nusxalarini yaratish hamda hodisalarga javob berish mexanizmlari kiradi. Agar himoyaning bir bosqichi buzilgan taqdirda ham boshqa himoya vositalari tahdidning tizim ichiga chuqur kirib borishining oldini oladi. Shu sababli zamonaviy tarmoq administratsiyasida aynan kompleks va ko‘p qatlamli himoya konsepsiyasi eng samarali yondashuv sifatida e’tirof etilmoqda.

So‘nggi yillarda sun’iy intellekt va mashinali o‘qitish texnologiyalarining rivojlanishi axborot xavfsizligini boshqarish tizimlariga ham sezilarli ta’sir ko‘rsatmoqda. Zamonaviy monitoring platformalari millionlab tarmoq hodisalarini real vaqt rejimida tahlil qilib, odatiy bo‘lmagan faollikni avtomatik aniqlash imkoniyatiga ega bo‘ldi. Bunday tizimlar administratorning ish yukini kamaytirish bilan birga tahdidlarni dastlabki bosqichdayoq aniqlash va ularga tezkor javob berish imkoniyatini yaratadi. Shu bilan birga, sun’iy intellekt asosidagi tizimlardan hujumchilar ham foydalanayotganligi sababli administratorlarning bilim va malakasini muntazam yangilab borish zamonaviy axborot xavfsizligining muhim talablaridan biri bo‘lib qolmoqda.

Kompyuter tarmoqlarini administratsiyalashda axborot xavfsizligini ta’minlash texnik vositalar, dasturiy yechimlar va tashkiliy choralarni yagona tizim sifatida qo‘llashni talab etadi. Aynan kompleks yondashuv tarmoq infratuzilmasining uzluksiz ishlashini ta’minlaydi, axborot resurslarini ishonchli himoya qiladi hamda tashkilot faoliyatining barqarorligini saqlab qolishda muhim omil bo‘lib xizmat qiladi. Shu bois zamonaviy tarmoq administratori axborot xavfsizligini kompyuter tarmog‘ining qo‘shimcha elementi emas, balki uning asosiy tarkibiy qismi sifatida baholashi va

barcha administrativ qarorlarni aynan xavfsizlik tamoyillari asosida qabul qilishi zarur.

Kompyuter tarmoqlarining murakkablashib borishi tarmoq administratorlari oldiga xavfsizlikni ta’minlashning yangi usullarini joriy etish vazifasini qo‘ymoqda. An’anaviy xavfsizlik vositalari bugungi kunda yuzaga kelayotgan murakkab kiberhujumlarning barchasiga qarshi yetarli darajada samarali emas. Shu sababli zamonaviy tarmoq administratsiyasi ko‘p qatlamli himoya tamoyili asosida tashkil etilib, apparat, dasturiy va tashkiliy vositalarning o‘zaro uyg‘un ishlashi ta’minlanadi. Administrator tarmoq infratuzilmasining barcha elementlari, jumladan serverlar, kommutatorlar, marshrutizatorlar, simsiz tarmoqlar, foydalanuvchi kompyuterlari va mobil qurilmalarni yagona xavfsizlik siyosati asosida boshqarishi zarur. Bunday yondashuv tarmoqning har bir nuqtasini nazorat qilish hamda ehtimoliy zaifliklarni o‘z vaqtida aniqlash imkonini beradi.

Tarmoq xavfsizligini ta’minlashda xavfsizlik devorlari (Firewall) eng asosiy himoya vositalaridan biri hisoblanadi. Zamonaviy Firewall tizimlari oddiy paketlarni filtrlash bilan cheklanib qolmay, ilovalar darajasida trafikni tahlil qilish, foydalanuvchilar faoliyatini nazorat qilish, zararli trafikni avtomatik bloklash hamda internet orqali amalga oshirilayotgan hujumlarni real vaqt rejimida aniqlash imkoniyatiga ega. Yangi avlod xavfsizlik devorlari (Next Generation Firewall – NGFW) Deep Packet Inspection texnologiyasi yordamida uzatilayotgan ma’lumotlar tarkibini chuqur tahlil qiladi. Natijada shifrlangan trafik tarkibidagi zararli faoliyat, noma’lum ilovalar yoki ruxsatsiz ulanishlar ham aniqlanadi. Administrator Firewall siyosatini ishlab chiqishda "minimal ruxsat" tamoyiliga amal qilishi, ya’ni foydalanuvchilarga faqat xizmat vazifalarini bajarish uchun zarur bo‘lgan resurslargagina kirish huquqini berishi lozim.

Masofadan turib ishlashning keng tarqalishi Virtual Private Network (VPN) texnologiyalarining ahamiyatini yanada oshirdi. VPN texnologiyasi ochiq internet tarmog‘i orqali uzatilayotgan ma’lumotlarni kuchli kriptografik algoritmlar yordamida shifrlaydi va foydalanuvchi bilan tashkilot tarmog‘i o‘rtasida himoyalangan aloqa kanalini hosil qiladi. Administrator VPN serverlarini sozlash jarayonida autentifikatsiya mexanizmlarini, sertifikatlarni boshqarish tizimini hamda foydalanuvchi vakolatlarini puxta tashkil qilishi zarur. Zamonaviy tashkilotlarda IPSec va SSL VPN texnologiyalaridan foydalanish keng tarqalgan bo‘lib, ular turli operatsion tizimlar va mobil qurilmalar bilan yuqori darajada moslashuvchan ishlaydi.

Tarmoq administratsiyasida foydalanuvchilarni boshqarish Active Directory, LDAP va boshqa katalog xizmatlari orqali amalga oshiriladi. Ushbu tizimlar barcha foydalanuvchi hisoblarini markazlashtirilgan holda boshqarish imkonini beradi. Administrator foydalanuvchilarning rollarini aniq belgilashi, guruh siyosatlari (Group Policy) yordamida xavfsizlik parametrlarini avtomatik qo‘llashi hamda keraksiz vakolatlarning berilishiga yo‘l qo‘ymasligi kerak. Markazlashtirilgan boshqaruv

nafaqat xavfsizlikni oshiradi, balki administratorning kundalik ishlarini avtomatlashtirishga ham xizmat qiladi. Shu bilan birga, ikki bosqichli autentifikatsiya (Multi-Factor Authentication) tizimining joriy etilishi foydalanuvchi paroli o‘g‘irlangan taqdirda ham tizimga noqonuniy kirishni sezilarli darajada kamaytiradi.

Tarmoq segmentatsiyasi zamonaviy administratsiyaning eng muhim elementlaridan biridir. Yirik korporativ tarmoqlarda barcha qurilmalarni bitta lokal tarmoqqa ulash xavfsizlik nuqtai nazaridan jiddiy xatolarga olib kelishi mumkin. Shu sababli administrator Virtual Local Area Network (VLAN) texnologiyasi yordamida tarmoqni alohida segmentlarga ajratadi. Masalan, buxgalteriya bo‘limi, serverlar zonasi, mehmonlar uchun Wi-Fi tarmog‘i va ishlab chiqarish uskunalari alohida segmentlarda ishlaydi. Segmentatsiya natijasida bitta segmentda yuzaga kelgan xavfsizlik hodisasi boshqa segmentlarga tarqalishining oldi olinadi. Bundan tashqari, VLAN lar o‘rtasidagi trafik ACL (Access Control List) qoidalari orqali qat’iy nazorat qilinadi.

Administratorning kundalik faoliyatida tarmoq monitoringi alohida o‘rin egallaydi. Monitoring tizimlari tarmoq uskunalarining ishlash holati, kanal yuklanishi, protsessor va operativ xotira bandligi, serverlarning ishlash ko‘rsatkichlari, foydalanuvchilar soni hamda xavfsizlik hodisalari haqida uzluksiz ma’lumot yig‘adi. SNMP, NetFlow, Syslog va Telemetry texnologiyalari administratorga tarmoqdagi barcha jarayonlarni kuzatish imkonini beradi. Ushbu ma’lumotlarning muntazam tahlili orqali uskunalardagi nosozliklar, trafikning g‘ayritabiiy o‘zgarishlari yoki ruxsatsiz ulanishlar dastlabki bosqichdayoq aniqlanadi. Bu esa katta miqdordagi zararlarning oldini olish imkonini yaratadi.

Kompyuter tarmoqlarida jurnallarni (log fayllarni) markazlashtirilgan tarzda yig‘ish va tahlil qilish ham zamonaviy xavfsizlikning muhim yo‘nalishlaridan hisoblanadi. Har bir server, marshrutizator, kommutator yoki xavfsizlik qurilmasi o‘z faoliyati davomida minglab hodisalarni qayd etadi. Ushbu log ma’lumotlari SIEM platformalarida jamlanib, o‘zaro bog‘liq ravishda tahlil qilinadi. Masalan, foydalanuvchi bir necha marta noto‘g‘ri parol kiritishi, keyin esa boshqa mamlakat IP manzilidan tizimga kirishga urinish holati avtomatik ravishda xavfli hodisa sifatida baholanadi. Administrator bunday ogohlantirishlarni tezkor ko‘rib chiqib, zarur choralarni ko‘rishi mumkin.

Axborot xavfsizligini ta’minlashda muntazam zaxira nusxalarini yaratish (Backup) va favqulodda vaziyatlardan tiklash (Disaster Recovery) rejalarini ishlab chiqish ham administratorning asosiy vazifalaridan biridir. Zaxira nusxalari nafaqat serverlardagi ma’lumotlarni, balki tarmoq qurilmalarining konfiguratsiyalarini ham o‘z ichiga olishi lozim. Amaliyotda "3-2-1" qoidasi keng qo‘llaniladi, ya’ni ma’lumotlarning kamida uchta nusxasi saqlanadi, ular ikki xil saqlash qurilmasida joylashtiriladi va ulardan bittasi boshqa geografik hududda yoki bulutli platformada

saqlanadi. Ushbu yondashuv tabiiy ofatlar, apparat nosozliklari yoki ransomware hujumlari natijasida ma’lumotlarning butunlay yo‘qolib ketishining oldini oladi.

Zamonaviy kompyuter tarmoqlarini administratsiyalashda avtomatlashtirish texnologiyalarining roli ham tobora ortib bormoqda. Administratorlar PowerShell, Python, Bash skriptlari hamda Ansible, Puppet va Terraform kabi avtomatlashtirish vositalari yordamida yuzlab server va tarmoq qurilmalarini qisqa vaqt ichida sozlash, konfiguratsiyalarni yangilash va xavfsizlik siyosatini avtomatik qo‘llash imkoniyatiga ega bo‘lmoqda. Avtomatlashtirish inson omili sababli yuzaga keladigan xatolarni kamaytiradi, boshqaruv samaradorligini oshiradi va xavfsizlik talablarining barcha qurilmalarda bir xil bajarilishini ta’minlaydi. Natijada administrator ko‘proq strategik xavfsizlik masalalariga e’tibor qaratishi mumkin bo‘ladi.

XULOSA

Xulosa qilib aytganda, kompyuter tarmoqlarini administratsiyalashda axborot xavfsizligini ta’minlash tarmoq infratuzilmasining barqaror va ishonchli ishlashini kafolatlovchi muhim omillardan biridir. Zamonaviy himoya vositalari, jumladan Firewall, VPN, tarmoq monitoringi, autentifikatsiya va segmentatsiya texnologiyalaridan kompleks foydalanish kiberxavflarning oldini olish hamda axborot resurslarini ishonchli himoyalashga xizmat qiladi. Shu bilan birga, tarmoq administratorlarining kasbiy malakasini muntazam oshirib borish, zamonaviy texnologiyalarni amaliyotga joriy etish va axborot xavfsizligi talablariga qat’iy rioya qilish kompyuter tarmoqlarining samaradorligi va xavfsizligini ta’minlashda muhim ahamiyat kasb etadi.

FOYDALANILGAN ADABIYOTLAR

1. Ismoilov A.A., Rasulov B.B. Kompyuter tarmoqlari. Toshkent: Cho‘lpon nomidagi NMIU, 2021. – 328 b.
2. Abdullayev Sh.A. Kompyuter tarmoqlarini loyihalash va administratsiyalash. Toshkent: Innovatsion rivojlanish nashriyoti, 2022. – 286 b.
3. Tojiyev R.X., Ergashev M.M. Axborot xavfsizligi asoslari. Toshkent: Fan va texnologiya, 2021. – 304 b.
4. Yuldashev Q.Q. Kompyuter tarmoqlarida axborot xavfsizligi. Toshkent: Tafakkur, 2020. – 276 b.
5. Karimov U.A. Tarmoq texnologiyalari va ularni boshqarish. Toshkent: O‘zbekiston, 2022. – 295 b.
6. Ahmedov N.R. Kiberxavfsizlik va tarmoq himoyasi. Toshkent: Yangi asr avlodi, 2023. – 312 b.