ZERO TRUST ARXITEKTURASI ASOSIDA KORPORATIV TARMOQ XAVFSIZLIGINI TA'MINLASH MASALALARI

Axmadaliyev Akramjon Rashidovich
Muhammad al-Xorazmiy nomidagi
Toshkent axborot texnologiyalari universiteti

Annotatsiya. Maqolada Zero Trust xavfsizlik arxitekturasining korporativ tarmoqlarga tatbiq etilishi masalalari yoritilgan. An'anaviy perimetr xavfsizligi modeli bilan solishtirilgan holda, mikrosegmentatsiya, doimiy autentifikatsiya va minimal huquqlar tamoyillariga asoslangan amaliy yondashuv taklif etilgan.

Kalit so'zlar: Zero Trust, mikrosegmentatsiya, autentifikatsiya, perimetr xavfsizligi, korporativ tarmoq, minimal huquqlar, identifikatsiya, masofaviy ish, bulut xavfsizligi, tarmoq segmentatsiyasi.

Korporativ tashkilotlarda masofaviy ishlash, bulutli texnologiyalardan foydalanish va tarmoq infratuzilmasining tarqoq xarakter kasb etishi an'anaviy perimetr xavfsizligi modelining samaradorligini pasaytirmoqda. Klassik yondashuvda tarmoq ichidagi foydalanuvchi va qurilmalarga avtomatik ishonch bildiriladi, biroq bu yondashuv ichki tahdidlar va kompromisga uchragan hisob yozuvlari orqali amalga oshiriladigan hujumlarga nisbatan zaif hisoblanadi.

Zero Trust ("hech kimga ishonmaslik") arxitekturasi ushbu muammoni hal qilishga yo'naltirilgan zamonaviy xavfsizlik modeli sifatida e'tirof etilmoqda. Ushbu model "hech qachon ishonma, doim tekshir" (never trust, always verify) tamoyiliga asoslanadi va tarmoq ichidagi yoki tashqarisidagi har qanday foydalanuvchi, qurilma yoki ilovaga nisbatan doimiy tekshiruvni talab qiladi.

Zero Trust arxitekturasini korporativ tarmoqqa tatbiq etishning asosiy tarkibiy qismlari quyidagilardan iborat: identifikatsiya va kirishni boshqarish (IAM), mikrosegmentatsiya, qurilma ishonchini baholash, doimiy monitoring va minimal huquqlar tamoyili (Principle of Least Privilege). Mikrosegmentatsiya tarmoqni kichik, izolyatsiyalangan segmentlarga bo'lish orqali hujumchining lateral harakatlanish (lateral movement) imkoniyatini cheklaydi.

Identifikatsiya va kirishni boshqarish tizimi ko'p faktorli autentifikatsiya (MFA), shartli kirish siyosatlari (Conditional Access) va atributga asoslangan kirishni boshqarish (ABAC) mexanizmlarini o'z ichiga oladi. Har bir kirish so'rovi foydalanuvchi identifikatori, qurilma holati, geografik joylashuv va xavf darajasi kabi ko'plab omillar asosida dinamik tarzda baholanadi.

Qurilma ishonchini baholash jarayonida endpoint detection and response (EDR) vositalari qurilmaning xavfsizlik holatini (operatsion tizim yangilanganligi, antivirus faolligi, zararli dasturlar mavjudligi) real vaqt rejimida tekshiradi. Agar qurilma belgilangan xavfsizlik mezonlariga javob bermasa, unga tarmoq resurslariga kirish huquqi cheklanadi yoki butunlay rad etiladi.

Mikrosegmentatsiyani amalga oshirishda dasturiy ta'minotga asoslangan tarmoqlar (Software-Defined Networking, SDN) va dasturiy ta'minotga asoslangan perimetr (Software-Defined Perimeter, SDP) texnologiyalaridan foydalanish tavsiya etiladi. Ushbu texnologiyalar har bir ilova va xizmat uchun alohida xavfsizlik perimetrini yaratish imkonini beradi, natijada hujumchi tarmoqning bir qismiga kirib olganda ham boshqa segmentlarga o‘tish imkoniyatidan mahrum bo‘ladi.

Zero Trust modelini joriy etishda korporativ tashkilotlar duch keladigan asosiy qiyinchiliklar mavjud infratuzilmani qayta loyihalash zarurati, xodimlar tomonidan yangi autentifikatsiya jarayonlariga moslashish muddati va boshlang‘ich investitsiya xarajatlarining yuqoriligi bilan bog‘liq. Shu sababli, bosqichma-bosqich joriy etish strategiyasi — avval eng muhim aktivlarni segmentatsiya qilish, so‘ngra butun tarmoqni qamrab olish — amaliy jihatdan maqbul hisoblanadi.

Xulosa qilib aytganda, Zero Trust arxitekturasi korporativ tarmoqlarda zamonaviy kiberhujumlarga, xususan ichki tahdidlar va lateral harakatlanishga qarshi samarali himoya mexanizmini ta'minlaydi. Mikrosegmentatsiya va doimiy autentifikatsiya tamoyillarini bosqichma-bosqich joriy etish tavsiya etiladi.

Foydalanilgan adabiyotlar.

1. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. NIST Special Publication 800-207, 2020.

2. Kindervag J. Build Security Into Your Network's DNA: The Zero Trust Network Architecture. Forrester Research, 2010.

3. Yan Z., Zhang P., Vasilakos A.V. A Survey on Trust Management for Internet of Things. Journal of Network and Computer Applications, 2014.

4. Allanov O.M. Korporativ tarmoqlarda foydalanishni boshqarish modellari. – Toshkent: TATU nashriyoti, 2022.

5. Garbis J., Chapman J.W. Zero Trust Security: An Enterprise Guide. Apress, 2021.

6. Юсупов С.Ю., Ғуломов Ш.Р. Тармоқ хавфсизлигида замонавий ёндашувлар: ўқув қўлланма. – Тошкент: «Aloqachi», 2021.