NOLINCHI ISHONCH (ZERO TRUST) ARXITEKTURASI ASOSIDA KORPORATIV TARMOQLARNI HIMOYALASH

UNIVERSITY OF BUSINESS AND SCIENCE
“aniq fanlar” kafedrasi katta o’qituvchisi
Hayitov Nasim To‘lqin o‘g‘li
Nasimhayitov1996@hmail.com

Annotatsiya

Ushbu maqolada korporativ tarmoqlarning axborot xavfsizligini ta'minlashda Nolinchi ishonch (Zero Trust) arxitekturasining o‘rni va ahamiyati tahlil qilingan. An'anaviy perimetrga asoslangan xavfsizlik yondashuvlarining kamchiliklari ko‘rib chiqilib, Zero Trust modelining asosiy tamoyillari yoritilgan. Shuningdek, korporativ tarmoqlarda Zero Trust arxitekturasini joriy etish bosqichlari, afzalliklari va amaliy qo‘llashdagi muammolar tahlil etilgan. Tadqiqot natijalariga ko‘ra, Zero Trust yondashuvi zamonaviy kiberxavfsizlik tahdidlariga qarshi samarali himoya mexanizmlaridan biri hisoblanadi.

Kalit so‘zlar: Zero Trust, kiberxavfsizlik, korporativ tarmoq, autentifikatsiya, avtorizatsiya, mikrosegmentatsiya, ko‘p faktorli autentifikatsiya, axborot xavfsizligi.

Kirish

Raqamli texnologiyalarning rivojlanishi, bulutli xizmatlarning ommalashuvi hamda masofadan ishlash tizimlarining keng qo‘llanilishi korporativ tarmoqlarning xavfsizligini ta'minlashda yangi yondashuvlarni talab qilmoqda. An'anaviy xavfsizlik tizimlari "ishonchli ichki tarmoq" va "ishonchsiz tashqi tarmoq" tamoyiliga asoslangan bo‘lib, foydalanuvchi ichki tarmoqqa kirgandan so‘ng unga katta darajada ishonch bildiriladi.

Biroq zamonaviy kiberhujumlar, ichki tahdidlar hamda zararli dasturlarning rivojlanishi ushbu modelning zaif tomonlarini namoyon qildi. Shu sababli "Hech qachon ishonma, har doim tekshir" ("Never Trust, Always Verify") tamoyiliga asoslangan Zero Trust arxitekturasi paydo bo‘ldi.

Zero Trust konsepsiyasi foydalanuvchi yoki qurilmaning joylashuviga qaramasdan har bir so‘rovni autentifikatsiya qilish, avtorizatsiya qilish va doimiy monitoringdan o‘tkazishni nazarda tutadi.

Zero Trust arxitekturasi tushunchasi

Zero Trust arxitekturasi ilk bor 2010-yilda Forrester Research kompaniyasi tahlilchisi John Kindervag tomonidan taklif etilgan. Mazkur modelning asosiy maqsadi tarmoq ichida yoki tashqarisida bo‘lishidan qat'i nazar, barcha foydalanuvchilar va qurilmalarga minimal darajadagi ruxsat berishdir.

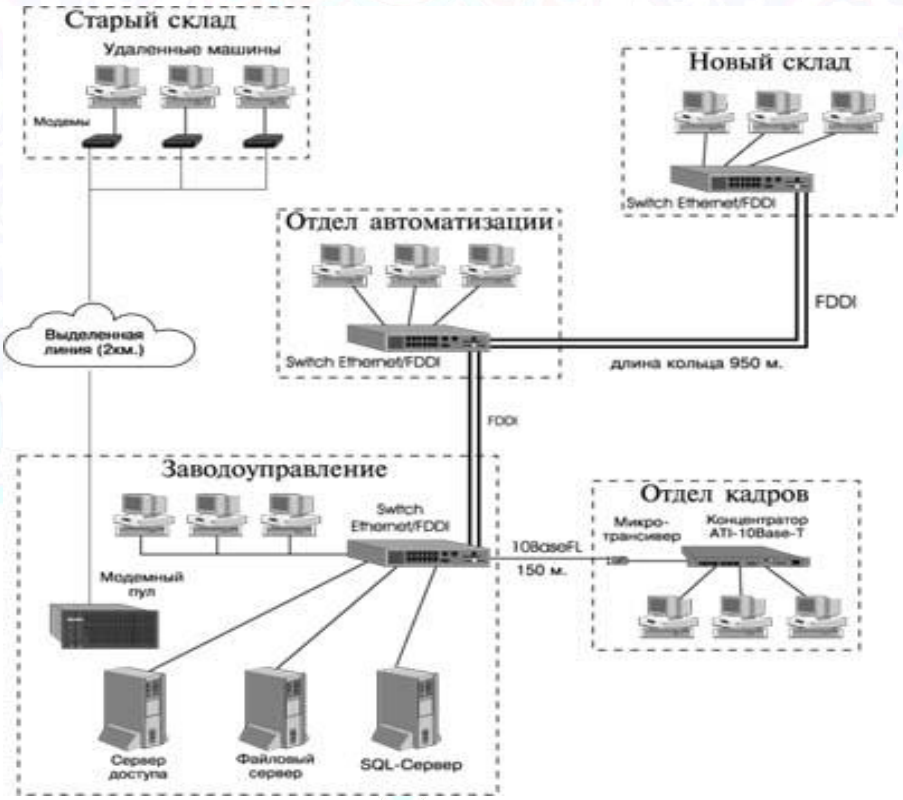
Zero Trust modeli quyidagi asosiy tamoyillarga asoslanadi:

- foydalanuvchilarni doimiy ravishda tekshirish;
- minimal imtiyozlar prinsipiga amal qilish;
- barcha qurilmalarni nazorat qilish;
- tarmoq resurslarini segmentatsiyalash;
- real vaqt rejimida monitoringni amalga oshirish;
- xavfsizlik siyosatini dinamik boshqarish.

An'anaviy xavfsizlik modeli va Zero Trust yondashuvining taqqoslanishi

Mezoni	An'anaviy model	Zero Trust modeli
Ishonch darajasi	Ichki tarmoqqa ishoniladi	Hech kimga avtomatik ishonilmaydi
Tekshiruv chastotasi	Bir martalik	Doimiy
Tarmoq tuzilishi	Perimetrga asoslangan	Mikrosegmentatsiyaga asoslangan
Kirish huquqi	Keng qamrovli	Minimal darajada
Monitoring	Cheklangan	Uzluksiz

Jadvaldan ko‘rinib turibdiki, Zero Trust yondashuvi zamonaviy tahdidlarga nisbatan ancha samarali himoyani ta'minlaydi.



Zero Trust arxitekturasining asosiy komponentlari

Identifikatsiya va autentifikatsiya

Zero Trust tizimining eng muhim elementlaridan biri foydalanuvchilarni ishonchli autentifikatsiya qilish hisoblanadi.

Bunda quyidagi usullar qo‘llaniladi:

- ko‘p faktorli autentifikatsiya (MFA);
- biometrik autentifikatsiya;
- yagona kirish tizimlari (SSO);
- identifikatsiyani boshqarish tizimlari (IAM).

Minimal imtiyozlar prinsipi

Foydalanuvchilarga faqat o‘z vazifalarini bajarish uchun zarur bo‘lgan resurslargagina kirish huquqi beriladi. Bu esa zararli harakatlar natijasida yuzaga keladigan xavflarni sezilarli darajada kamaytiradi.

Mikrosegmentatsiya

Mikrosegmentatsiya tarmoqni kichik himoyalangan segmentlarga ajratishni nazarda tutadi. Natijada tajovuzkor bir segmentga kirgan taqdirda ham butun tizim bo‘ylab harakatlana olmaydi.

Mikrosegmentatsiyaning afzalliklari:

- lateral harakatlarni cheklash;
- tahdidlarni tezkor lokalizatsiya qilish;
- xavfsizlik siyosatini moslashuvchan boshqarish.

Uzluksiz monitoring

Zero Trust modelida foydalanuvchi faoliyati doimiy ravishda kuzatib boriladi.

Monitoring quyidagilarni o‘z ichiga oladi:

- tarmoq trafigini tahlil qilish;
- qurilmalar holatini baholash;
- foydalanuvchi xatti-harakatlarini monitoring qilish;
- xavf darajasini dinamik hisoblash.

Korporativ tarmoqlarda Zero Trust arxitekturasini joriy etish bosqichlari

1-bosqich. Muhim resurslarni aniqlash

Tashkilot uchun eng muhim bo‘lgan aktivlar aniqlanadi:

- ma'lumotlar bazalari;
- serverlar;
- biznes ilovalar;
- bulutli xizmatlar.

2-bosqich. Tarmoq infratuzilmasini tahlil qilish

Mavjud tarmoq arxitekturasi o‘rganiladi va zaif nuqtalar aniqlanadi.

3-bosqich. Identifikatsiyani boshqarish tizimlarini joriy etish

IAM va MFA texnologiyalari tatbiq etiladi.

4-bosqich. Mikrosegmentatsiyani amalga oshirish

Tarmoq xavfsizlik zonalariga ajratiladi.

5-bosqich. Monitoring va tahlil tizimlarini joriy etish

SIEM va sun'iy intellekt asosidagi monitoring vositalari qo‘llaniladi.

Zero Trust modelining afzalliklari

Zero Trust arxitekturasini joriy etish quyidagi natijalarga erishish imkonini beradi:

- ichki tahdidlardan himoyalanish;
- ma'lumotlarning sizib chiqish xavfini kamaytirish;
- masofaviy xodimlar faoliyatini xavfsiz tashkil etish;
- bulutli xizmatlardan xavfsiz foydalanish;
- normativ talablar va standartlarga muvofiqlikni ta'minlash;
- kiberhujumlarning tarqalishini cheklash.

Zero Trust arxitekturasini joriy etishdagi muammolar

Mazkur modelni amaliyotga tatbiq etishda ayrim qiyinchiliklar ham mavjud:

- joriy etish xarajatlarining yuqoriligi;
- eski infratuzilmalar bilan integratsiya muammolari;
- malakali mutaxassislar yetishmasligi;
- foydalanuvchilarning qarshiligi;
- xavfsizlik siyosatini to‘g‘ri sozlash zarurati.

Shunga qaramasdan, mazkur muammolar Zero Trust modelining afzalliklarini kamaytirmaydi.

Xulosa

Zero Trust arxitekturasi zamonaviy korporativ tarmoqlarni himoyalashning istiqbolli yondashuvlaridan biri hisoblanadi. "Hech qachon ishonma, har doim tekshir" tamoyiliga asoslangan ushbu model ichki va tashqi tahdidlarga qarshi samarali himoyani ta'minlaydi.

Tadqiqot natijalari shuni ko‘rsatadiki, mikrosegmentatsiya, ko‘p faktorli autentifikatsiya hamda uzluksiz monitoring kabi mexanizmlarni joriy etish korporativ tarmoqlarning xavfsizlik darajasini sezilarli oshiradi. Kelgusida sun'iy intellekt

texnologiyalarini Zero Trust tizimlari bilan integratsiya qilish kiberxavfsizlikni yanada takomillashtirish imkonini beradi.

Foydalanilgan adabiyotlar

1. Kindervag J. *Build Security Into Your Network's DNA: The Zero Trust Network Architecture*. Forrester Research, 2010.
2. Rose S., Borchert O., Mitchell S., Connelly S. *Zero Trust Architecture*. NIST Special Publication 800-207, 2020.
3. Stallings W. *Network Security Essentials: Applications and Standards*. Pearson Education, 2017.
4. Whitman M., Mattord H. *Principles of Information Security*. Cengage Learning, 2022.
5. Gilman E., Barth D. *Zero Trust Networks: Building Secure Systems in Untrusted Networks*. O'Reilly Media, 2017.
6. Scarfone K., Mell P. *Guide to Intrusion Detection and Prevention Systems*. NIST, 2007.
7. Microsoft. *Zero Trust Deployment Guide*, 2024.
8. Cisco Systems. *Zero Trust Security Framework*, 2024.
9. Palo Alto Networks. *The Essential Guide to Zero Trust Security*, 2023.
10. IBM Security. *Zero Trust Strategy and Implementation Guide*, 2024.
11. ENISA. *Threat Landscape Report*, 2024.
12. ISO/IEC 27001:2022 Information Security Management Systems.
13. NIST Cybersecurity Framework 2.0, 2024.
14. Check Point Research. *Cyber Security Report*, 2025.
15. O‘zbekiston Respublikasining axborot xavfsizligi va kiberxavfsizlik sohasiga oid normativ-huquqiy hujjatlari.