RESEARCH ON METHODS OF IMPLEMENTING “ZERO TRUST” ARCHITECTURE IN CYBERSECURITY

Maxsudov Azamxon Yunusxo‘ja o‘g‘li
Master’s Student, Information Security Fergana State Technical University
Tel: +998911612545
Turdimatov Mamirjon Mirzayevich
Associate Professor, Department of Software Engineering and Cybersecurity, PhD (Technical Sciences) Fergana State Technical University
Tel: +998916762211

Abstract: Zero Trust architecture is becoming a strategic principle of modern information security. It promotes an approach based on continuous verification, least privilege, and constant monitoring instead of implicit trust. This article provides an in-depth analysis of the core principles of the Zero Trust model, its technological solutions, the practices of leading companies, implementation stages, and the prospects for its adoption in Uzbekistan.

Keywords: Zero Trust, authentication, user control, microsegmentation, cybersecurity, monitoring.

KIBERXAVFSIZLIKDA “ZERO TRUST” ARXITEKTURASINING QO'LLASH USULLARINI TADQIQI

1) Maxsudov Azamxon Yunusxo’ja og’li
Farg’ona davlat texnika universiteti “Axborot xavfsizligi yo’nalishi magistranti
+998911612545
2) Turdimatov Mamirjon Mirzayevich
Farg’ona davlat texnika universiteti “Dasturiy injiniring va kiberxavfsizlik” kafedrasi donsenti t.f.n

+998916762211

Annotatsiya: Zero Trust arxitekturasi zamonaviy axborot xavfsizligining strategik tamoyiliga aylanib bormoqda. U doimiy tekshirish, minimal imtiyozlar va shubhasizlik o‘rniga doimiy nazorat yondashuvini taklif qiladi. Ushbu maqolada Zero Trust modelining asosiy printsiplari, texnologik yechimlari, ilg‘or kompaniyalar tajribalari, amaliyotda qo‘llash bosqichlari va O‘zbekistondagi joriy etish imkoniyatlari chuqur tahlil qilinadi.

Kalit so‘zlar: Zero Trust, autentifikatsiya, foydalanuvchi nazorati, mikrosegmentatsiya, kiberxavfsizlik, monitoring.

Kirish. Kiberxavfsizlik zamonaviy dunyoda tobora muhim ahamiyat kasb etmoqda. Raqamli transformatsiya, bulutli texnologiyalar va masofaviy ish muhitlarining keng tarqalishi tashkilotlar uchun yangi kiberxavf-xatarlarni keltirib chiqarmoqda. An’anaviy xavfsizlik yondashuvlari, masalan, tarmoq perimetriga asoslangan himoya modellari, zamonaviy kiberhujumlar oldida yetarli samaradorlikni ta’minlay olmayapti. Ushbu sharoitda “Zero Trust” arxitekturasi kiberxavfsizlik sohasida inqilobiy yondashuv sifatida paydo bo‘ldi.

Zero Trust falsafasi “hech kimga ishonma, har doim tekshir” tamoyiliga asoslanadi. Bu yondashuv tarmoq ichidagi yoki tashqarisidagi har qanday foydalanuvchi, qurilma yoki ilovaga avtomatik ishonch bildirishni rad etadi. Har bir kirish so‘rovi doimiy ravishda autentifikatsiya qilinadi, avtorizatsiya qilinadi va kontekstual tahlil qilinadi. Zero Trustning asosiy maqsadi tashkilotlarni ichki va tashqi xavf-xatarlardan himoya qilish, shu bilan birga moslashuvchanlik va samaradorlikni ta’minlashdir.

Ushbu maqola Zero Trust arxitekturasining asosiy tamoyillari, qo‘llanilishi va joriy etish usullarini keng ko‘lamda tahlil qiladi. Maqolaning maqsadi tashkilotlarga ushbu yondashuvni o‘z infratuzilmalarida samarali joriy etish bo‘yicha amaliy tavsiyalar berish va kiberxavfsizlik sohasidagi so‘nggi tendensiyalarni yoritishdir. Maqola

quyidagi bo‘limlardan iborat: Zero Trustning asoslari, qo‘llanilishi, joriy etish usullari, kelajakdagi tendensiyalar va xulosa.

So‘nggi yillarda raqamli texnologiyalarning keng joriy etilishi kiberxavfsizlik tahdidlarini sezilarli darajada oshirdi. Klassik perimetr asosidagi xavfsizlik yondashuvi — ya'ni ichki tarmoqda joylashgan foydalanuvchiga avtomatik ishonch tamoyili — bugungi zamonaviy tahdidlar oldida samarasiz bo‘lib qoldi. Zero Trust (Nol ishonch) arxitekturasi esa bu muammoni “hech kimga ishonma, hammani tekshir” printsipi asosida hal qiladi. Zero Trust konsepsiyasi xavfsizlikni foydalanuvchi joylashuvi, qurilma holati, kirish vaqti, kontekstual ma’lumotlar asosida doimiy baholashni talab qiladi. Ushbu maqola Zero Trust arxitekturasi qanday ishlashi, qanday texnologiyalarga tayanishi va uni tashkilotlarda qanday tatbiq etish mumkinligini batafsil yoritadi.

Zamonaviy kibertahdidlarning ortishi bilan an’anaviy "ishonchli perimeter" modeli samaradorligini yo‘qotmoqda. Zero Trust (nol ishonch) arxitekturasi – bu har qanday kirish so‘rovini, hatto tashqi emas, balki tarmoq ichidan bo‘lganlarini ham, avtomatik ravishda ishonmaydi va qat’iy tekshiruvdan o‘tkazadi. Ushbu maqolada Zero Trust tamoyillari, qo‘llash usullari, amaliy misollar va kelajakdagi istiqbollari tahlil qilinadi.

Adabiyotlar tahlili va ilmiy-asosiy yondashuv. Zero Trust modeli ilk bor 2010-yilda Forrester tadqiqotchisi Jon Kindervag tomonidan ilgari surilgan. Unga ko‘ra, hech bir foydalanuvchiga, hatto ichki tarmoq foydalanuvchisiga ham avtomatik tarzda ishonish mumkin emas.

Zero Trust arxitekturasi kiberxavfsizlikda yangi paradigma sifatida 2000-yillarning oxirida Forrester Research tomonidan joriy etilgan. Ushbu yondashuv “hech kimga ishonma, har doim tekshir” tamoyiliga asoslanadi. Zero Trust tarmoq ichidagi yoki tashqarisidagi hech bir sub’ektga (foydalanuvchi, qurilma yoki ilova) avtomatik ishonch bildirilmasligini talab qiladi. Har bir kirish so‘rovi kontekstual tahlil, identifikatsiya va doimiy monitoring asosida tekshiriladi.

Zero Trustning asosiy tamoyillari quyidagilardan iborat:

Doimiy tekshiruv: Har bir foydalanuvchi va qurilma har bir kirish so‘rovida autentifikatsiya qilinadi.

Eng kam imtiyozlar prinsipi: Foydalanuvchilar faqat o‘z vazifalarini bajarish uchun zarur bo‘lgan ruxsatlarga ega bo‘ladi.

Tarmoq segmentatsiyasi: Tarmoq kichik segmentlarga bo‘linadi, bu esa xavfli harakatlarni cheklaydi.

Doimiy monitoring: Barcha tarmoq faoliyati real vaqtda kuzatiladi va tahlil qilinadi.

Zero Trust an’anaviy xavfsizlik modellaridan tubdan farq qiladi. An’anaviy modellar tarmoq perimetriga asoslanib, tarmoq ichidagi barcha sub’ektlarni ishonchli deb hisoblaydi. Zero Trust esa bunday taxminni rad etadi va har bir so‘rovni mustaqil ravishda tekshiradi. Bu yondashuv zamonaviy muhitlarda, masalan, bulutli infratuzilmalarda va masofaviy ish joylarida, an’anaviy modellar yetishmaydigan joylarda samarali ishlaydi.

2.1. Zero Trustning qo‘llanilishi va asosiy tamoyillar:

Zero Trust arxitekturasi kiberxavfsizlikning turli sohalarda qo‘llanilishi mumkin bo‘lgan moslashuvchan yondashuv sifatida ishlab chiqilgan. U tarmoq xavfsizligidan tortib bulutli muhitlar, qurilmalar va ilovalargacha bo‘lgan keng doiradagi infratuzilmalarda samarali ishlaydi. Quyida Zero Trustning asosiy qo‘llanilish sohalari ko‘rib chiqiladi.

Tarmoq xavfsizligida Zero Trust

Tarmoq xavfsizligi Zero Trust arxitekturasining eng muhim qo‘llanilish sohasidir. An’anaviy tarmoq xavfsizligi tarmoq perimetriga asoslangan bo‘lib, tashqi xavf-xatarlarni bloklashga qaratilgan edi. Biroq, ichki xavf-xatarlarning ko‘payishi va tarmoq chegaralarining xiralashishi tufayli Zero Trust yangi yondashuvni talab qiladi.

Mikrosegmentatsiya Zero Trustning tarmoq xavfsizligidagi asosiy usullaridan biridir. Bu usul tarmoqni kichik, mustaqil segmentlarga bo‘lishni anglatadi, bunda har bir segment o‘ziga xos xavfsizlik siyosatlariga ega bo‘ladi. Agar bir segmentga xavf-xatar kirib kelsa, u boshqa segmentlarga tarqalmaydi. Masalan, korporativ tarmoqda moliya bo‘limi va marketing bo‘limi uchun alohida segmentlar yaratilishi mumkin, bu esa ma'lumotlarga ruxsatsiz kirishni cheklaydi.

Tarmoqqa kirishni boshqarish (Network Access Control, NAC) Zero Trustning yana bir muhim komponentidir. NAC tarmoqqa ulanadigan har bir qurilma va foydalanuvchining identifikatsiyasini va xavfsizlik holatini tekshiradi. Masalan, agar xodimning qurilmasida so‘nggi xavfsizlik yangilanishlari o‘rnatilmagan bo‘lsa, unga tarmoqqa kirish taqiqlanadi.

Bulutli muhitlarda Zero Trust

Bulutli texnologiyalarning keng tarqalishi Zero Trust arxitekturasining bulutli muhitlarda qo‘llanilishini dolzarb qildi. Bulutli xizmatlar, masalan, SaaS (Software as a Service), PaaS (Platform as a Service) va IaaS (Infrastructure as a Service), tashkilotlarga moslashuvchanlik taqdim etadi, lekin bir vaqtning o‘zida yangi xavf-xatarlarni keltirib chiqaradi.

Bulutli muhitlarda Zero Trust autentifikatsiya va shifrlashga alohida e’tibor beradi. Masalan, ko‘p faktorli autentifikatsiya (MFA) har bir foydalanuvchi uchun majburiydir. Bundan tashqari, ma'lumotlar bulutda saqlanayotganda yoki uzatilayotganda doimiy shifrlanadi. Zero Trust bulutli xizmatlarda API xavfsizligini ta’minlashga ham yordam beradi, chunki API’lar ko‘pincha hujumlarning asosiy nishoniga aylanadi.

Qurilma xavfsizligida Zero Trust

Zamonaviy tashkilotlarda IoT (Internet of Things) qurilmalari va BYOD (Bring Your Own Device) siyosatlari keng tarqalgan. Bu esa qurilma xavfsizligini ta’minlashni yanada murakkablashtiradi. Zero Trust ushbu muammoni hal qilish uchun har bir

qurilmani doimiy monitoring qilishni va uning xavfsizlik holatini tekshirishni talab qiladi.

Masalan, agar xodim shaxsiy noutbukidan korporativ tarmoqqa kirishga harakat qilsa, Zero Trust tizimi avval ushbu qurilmaning operatsion tizimi, xavfsizlik dasturlari va tarmoq ulanishini tekshiradi. Agar qurilma talab qilinadigan xavfsizlik standartlariga javob bermasa, kirish taqiqlanadi.

Ilovalar va ma'lumotlar xavfsizligi

Zero Trust ma'lumotlar xavfsizligiga alohida e’tibor beradi. Ma'lumotlarni shifrlash va tokenizatsiya kabi usullar orqali Zero Trust nozik ma'lumotlarni himoya qiladi. Masalan, ma'lumotlar bazasidagi shaxsiy ma'lumotlar tokenlashtiriladi, ya’ni haqiqiy ma'lumotlar o‘rniga maxsus tokenlar ishlatiladi, bu esa ma'lumotlar o‘g‘irlangan taqdirda ularni foydasiz qiladi.

API xavfsizligi ham Zero Trustning muhim qismidir. Zamonaviy ilovalar ko‘pincha API’lar orqali bir-biri bilan aloqa qiladi, va Zero Trust har bir API so‘rovini autentifikatsiya qilish va avtorizatsiya qilishni talab qiladi.

Zero Trustni joriy etish usullari

Zero Trust arxitekturasini tashkilotda joriy etish murakkab va ko‘p bosqichli jarayon bo‘lib, unda infratuzilma tahlili, siyosatlar ishlab chiqish va texnologik yechimlar tanlash talab qilinadi. Quyida Zero Trustni joriy etishning asosiy bosqichlari va usullari ko‘rib chiqiladi.

Joriy etish bosqichlari

Infratuzilma tahlili: Zero Trustni joriy etishdan oldin tashkilotning mavjud tarmoq infratuzilmasi, qurilmalari, ilovalari va ma'lumot oqimlari tahlil qilinadi. Bu jarayon tashkilotning zaif nuqtalarini aniqlash va xavf-xatarlarni baholashga yordam beradi.

Siyosatlar ishlab chiqish: Zero Trust doirasida aniq xavfsizlik siyosatlari ishlab chiqiladi. Masalan, qaysi foydalanuvchilar qaysi resurslarga kirishi mumkinligi aniqlanadi va eng kam imtiyozlar prinsipi qo‘llaniladi.

Texnologik yechimlar tanlash: Zero Trustni amalga oshirish uchun maxsus texnologiyalar, masalan, SIEM (Security Information and Event Management), IAM (Identity and Access Management) va SDP (Software-Defined Perimeter) tizimlari tanlanadi.

Amaliy misollar va case study-lar

Zero Trustni muvaffaqiyatli joriy etgan tashkilotlar orasida yirik korporatsiyalar, masalan, Google va Microsoft misol keltiriladi. Google o‘zining “BeyondCorp” tashabbusi orqali Zero Trustni joriy etdi, bu esa xodimlarga tarmoq perimetrisiz, faqat autentifikatsiya va avtorizatsiya asosida resurslarga kirish imkonini berdi. Kichik va o‘rta bizneslar ham Zero Trustni qabul qilmoqda, masalan, bulutli xizmatlardan foydalanadigan startaplar MFA va mikrosegmentatsiyani joriy etmoqda.

Joriy etishdagi qiyinchiliklar

Zero Trustni joriy etishda bir qator qiyinchiliklar mavjud, masalan:

Moliyaviy xarajatlar: Zero Trust texnologiyalari va xodimlar malakasini oshirish qimmatga tushadi.

Tashkiliy o‘zgarishlar: Xodimlar va jarayonlar yangi xavfsizlik siyosatlariga moslashishi kerak.

Texnik murakkablik: Mavjud infratuzilmani Zero Trust tamoyillariga moslashtirish ko‘p vaqt talab qiladi.

Bu qiyinchiliklarni bartaraf etish uchun tashkilotlar bosqichma-bosqich joriy etish strategiyasini qo‘llashi, kiberxavfsizlik bo‘yicha mutaxassislarni jalb qilishi va xodimlarni doimiy ravishda o‘qitishi tavsiya etiladi.

Zero Trustning kelajagi va rivojlanish tendensiyalari

Zero Trust arxitekturasi doimiy ravishda rivojlanmoqda va kelajakda kiberxavfsizlik sohasida yanada muhim o‘rin egallaydi. Quyida Zero Trustning kelajakdagi tendensiyalari ko‘rib chiqiladi.

Sun’iy intellekt va mashinaviy o‘qitish

Sun’iy intellekt (AI) va mashinaviy o‘qitish Zero Trust tizimlarini yanada aqlli va moslashuvchan qilmoqda. Masalan, AI tarmoq faoliyatini real vaqtda tahlil qilib, g‘ayritabiiy harakatlarni aniqlay oladi. Bu xavf-xatarlarni tezroq aniqlash va ularga javob berish imkonini beradi.

Kvant hisoblash

Kvant hisoblashning rivojlanishi kiberxavfsizlikda yangi imkoniyatlar va xavf-xatarlarni keltirib chiqarmoqda. Zero Trust arxitekturasi kvant hisoblashga asoslangan shifrlash algoritmlarini integratsiya qilish orqali kelajakdagi xavf-xatarlarga tayyorlanmoqda.

Global qonunchilik va standartlar

Zero Trust arxitekturasi global qonunchilik va standartlarga, masalan, GDPR (General Data Protection Regulation) va NIST 800-207 ga moslashmoqda. Bu tashkilotlarga xalqaro talablarga rioya qilishda yordam beradi.

- **Doimiy tekshirish (Continuous verification):** Har bir harakat doimiy ravishda qayta tekshiriladi.
- **Minimal imtiyoz (Least privilege):** Foydalanuvchi faqat kerakli resursga cheklangan kirish huquqiga ega bo‘ladi.
- **Konfiguratsiyalarning monitoringi:** Barcha qurilmalar va foydalanuvchilar holati doimiy nazoratda bo‘ladi.
- **Mikrosegmentatsiya:** Tarmoq segmentlarga bo‘linadi, har bir segment alohida nazorat ostida bo‘ladi.

2.2. Ilmiy manbalar

- NIST SP 800-207 (2020) standarti Zero Trust arxitekturasi bo‘yicha ilmiy asoslangan modelni belgilaydi.
- Google’ning **BeyondCorp** modeli, Microsoft’ning **Zero Trust Maturity Model**i — yirik korporatsiyalar tajribasi.
- Forrester va Gartner hisobotlari orqali tahdidlar dinamikasi, amaliy natijalar va joriy etishdagi muammolar tahlil qilinadi.

Texnologik komponentlar va infrastruktura. Zero Trust arxitekturasi quyidagi texnologik komponentlarga tayanadi:

3.1. Foydalanuvchi va qurilma identifikatsiyasi

- Multi-factor Authentication (MFA): Parol + biometrik ma’lumot + qurilma.
- Endpoint Detection and Response (EDR): Qurilma holatini baholash va monitoring qilish.

3.2. Kirish nazorati va ruxsat boshqaruvi

- Identity and Access Management (IAM): Foydalanuvchi roli, joylashuvi, qurilmasiga asoslangan ruxsatlar.
- Privileged Access Management (PAM): Maxsus vakolatli foydalanuvchilar harakati ustidan nazorat.

3.3. Mikrosegmentatsiya va tarmoq xavfsizligi

- Software-defined Perimeter (SDP): Ichki tarmoq resurslari foydalanuvchi ehtiyojiga mos taqdim etiladi.
- Firewalls va NAC (Network Access Control): Har bir tarmoq segmentiga kirishni nazorat qiladi.

3.4. Doimiy monitoring va tahlil

- Security Information and Event Management (SIEM): Hodisalar tahlili.
- User and Entity Behavior Analytics (UEBA): Foydalanuvchi odatidan chetga chiqishlar aniqlanadi.

`Qo‘llash usullari va joriy etish bosqichlari. Zero Trust’ni joriy etish 5 bosqichdan iborat bo‘lishi mumkin:

1. Tarmoq va resurslar inventarizatsiyasi: Hamma foydalanuvchi va qurilmalarni aniqlash.

2. Ruxsat darajalarini qayta baholash: Minimal imtiyoz prinsipiga moslashtirish.

3. Autentifikatsiya tizimini kuchaytirish: MFA va riskga asoslangan autentifikatsiya joriy etish.

4. Tarmoq segmentatsiyasi: Har bir xizmatni alohida xavfsizlik chegarasi bilan ajratish.

5. Monitoring va takomillashtirish: Zero Trust modelining samaradorligini doimiy baholash.

Tajriba va amaliy misollar

5.1. Google BeyondCorp

Google o‘zining ichki tarmog‘ini butunlay Zero Trust printsipiga o‘tkazgan. Natijada xodimlar dunyoning istalgan nuqtasidan xavfsiz ulanish imkoniyatiga ega bo‘lgan.

5.2. Microsoft Zero Trust model

Microsoft joriy etgan Zero Trust modelida barcha foydalanuvchilarning harakati real vaqt rejimida monitoring qilinadi, va kirish kontekst asosida taqdim etiladi.

5.3. O‘zbekistondagi imkoniyatlar

Davlat axborot tizimlari, moliyaviy tashkilotlar va yirik korporatsiyalar Zero Trust modelini qisman qo‘llay boshlagan. Lekin infrastrukturaviy muammolar, malakali kadrlar yetishmasligi va moliyaviy cheklovlar hali to‘liq joriy etishga to‘sqinlik qilmoqda.

Xulosa va takliflar. Zero Trust — kiberxavfsizlikda yangi davrni boshlab bergan konsepsiyadir. U quyidagi afzalliklarga ega: Zero Trust arxitekturasi zamonaviy

kibertahdidlarga qarshi eng samarali yondashuvlardan biridir. U tashqi va ichki tahdidlarni bartaraf etishda katta samara beradi, ammo uni to‘g‘ri joriy etish uchun tashkilot texnologik, moliyaviy va kadrlar jihatidan tayyor bo‘lishi kerak. Kelajakda sun’iy intellekt va mashina o‘rganish texnologiyalari Zero Trust tizimlarini yanada avtomatlashtirib, himoyani yanada mustahkamlaydi.

- Tahdidlarni real vaqt rejimida aniqlash;
- Foydalanuvchi faoliyati ustidan to‘liq nazorat;
- Ichki hujumlar (insayder tahdidlar)ga qarshi himoya;
- Masofaviy ish tizimlari uchun ideal model.

Takliflar:

1. O‘zbekiston tashkilotlarida Zero Trust joriy etilishi uchun hukumat darajasida siyosat ishlab chiqilishi lozim.

2. Mahalliy IT mutaxassislarini Zero Trust arxitekturasi bo‘yicha malakasini oshirish.

3. Davlat axborot tizimlarida tajriba loyihalari asosida Zero Trustni sinovdan o‘tkazish.

Foydalanilgan adabiyotlar

1. Kindervag J. “Build Security Into Your Network’s DNA: The Zero Trust Network Architecture”, Forrester Research, 2010.

2. NIST SP 800-207, “Zero Trust Architecture”, 2020.

3. Google BeyondCorp Whitepaper, 2014.

4. Microsoft Zero Trust Adoption Report, 2022.

5. Gartner. “Top Security Trends”, 2023.

6. Anderson R. “Security Engineering”, Wiley, 2020.

7. SANS Institute. “Zero Trust Security for Enterprises”, 2021.

8. Cisco. “Implementing Zero Trust Architecture”, 2022.