**O‘ZBEKISTON RESPUBLIKASI**

**RAQAMLI TEXNOLOGIYALARI VAZIRLIGI**

**MUHAMMAD AL-XORAZMIY NOMIDAGI**

**TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI**



***“*Axborotlarni izlash va ajratib olish*”***

**fanidan**

**Mustaqil ishi 1**

**Guruh:** 801-25

**Bajardi:** Savriyev S.

**Qabul qildi:** Abdug‘aniyev M.

**Toshkent 2025**

**Mavzu:** Kiberhujumlardan himoya qilishda axborot ajratish roli.

Mundarija:

1. Kiberhujumlar, internetdan bo’ladigan kiberhujumlar va ularning turlari. 3

2. Zamonaviy kiber tahdidlar tendensiyalari. 5

3. Kiberhujumlarning ijtimoiy-iqtisodiy oqibatlari. 7

4. Axborotni ajratish (segmentation) tushunchasi. 10

5. Tarmoq segmentatsiya turlari: 11

5.1 Fizik(Jismoniy) segmentatsiya (Physical Segmentation)  
 5.2. Mantiqiy segmentatsiya (Logical Segmentation)  
 5.3. Mikrosegmentatsiya (Microsegmentation)

6. Segmentatsiya samaradorligini va foydalari 14

7. Xulosa. 15

8. Foydalanilgan adabiyotlar va saytlar ro’yhati. 16

**1.** Kiberhujumlar har qachongidan ham maqsadli, doimiy va murakkab bo'lib qoldi.Tarmoqlarni ushbu tahdidlardan himoya qilish ongni o'zgartirishni talab qiladi - bu tarmoq segmentatsiyasini xavfsizlikning asosiy strategiyasi sifatida qabul qiladi. Tashkilotlar faqat perimetr himoyasiga tayanishdan ko'ra, xavfsizlikni to'g'ridan-to'g'ri tarmoq tuzilishiga o'rnatishlari, buzilishlarga tayyorgarlik ko'rishlari va ularning mumkin bo'lgan ta'sirini minimallashtirishlari kerak.

**Zamonaviy kibertahdidlar manzarasi:** So'nggi yillarda tahdidlar manzarasi keskin o'zgardi, tajovuzkorlar tarmoqlarga kirib borish va tizimlar bo'ylab lateral harakatlanish uchun yanada murakkab usullardan foydalanadilar. [Tashkilotlarning 90%](https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024" \l "section-master-oc526b) dan ortig'i hozirda kamida bitta hujum yo'liga duchor bo'lmoqda - 80% muhim aktivlarni fosh qiladigan yo'llarga ega. Boshqacha qilib aytganda, aksariyat tashkilotlar yuqori qiymatli aktivlarga erishish uchun ichki tarmoq yo'llaridan foydalanadigan tajovuzkorlarga nisbatan zaifdir. Ilg'or doimiy tahdidlar va insayder hujumlar tobora kengayib bormoqda, bu esa an'anaviy perimetrga asoslangan himoyalarni yetarli darajada emasligini anglatadi. Bunday yuqori xavfli muhitda tekis tarmoq arxitekturasiga tayanish tashkilotlarni himoyasiz qoldiradi. Tarmoq segmentatsiyasi lateral harakatni cheklash va izolyatsiya qilingan zonalarda potentsial buzilishlarni o'z ichiga olgan holda ushbu muammolarni hal qiladi. Ushbu strategiya nafaqat hujum darajasini pasaytiradi, balki tarmoq faoliyatining qimmatli ko'rinishini ham ta'minlaydi, bu esa tahdidlarni tezroq aniqlash va javob berishga imkon beradi.

**Kiberhujum turlari:**

**1) DDoS hujumlari – Saytni ishdan chiqaradigan xavf**

DDoS (Distributed Denial of Service) hujumi — bu veb-sayt yoki onlayn xizmatni vaqtinchalik yoki butunlay ishdan chiqarish uchun qilinadigan hujum. Hujumchilar buzilgan qurilmalar orqali bir saytga birdaniga juda katta hajmda so‘rov (trafik) yuborishadi. Natijada sayt ortiqcha yuklama sabab ishlashdan to‘xtab qoladi yoki judasekinlashadi.

**2) Fishing (Phishing) – Aldov orqali ma’lumot o‘g‘irlash**

Fishing — jinoyatchilar tomonidan odamlarni aldash orqali parol, karta raqami yoki boshqa shaxsiy ma’lumotlarni qo‘lga kiritish usuli. Ular o‘zlarini bank yoki ishonchli tashkilot nomidan xabar yuborib, sizdan maxfiy ma’lumot so‘rashadi. Bu ko‘pincha telefon qo‘ng‘iroq, e-mail, SMS yoki ijtimoiy tarmoqlarda bo‘ladi.

**3) Backdoor hujumlari – Tizimga yashirin kirish**

Backdoor — dastur yoki tizimdagi yashirin “eshik” bo‘lib, jinoyatchilar bunga kirib, foydalanuvchining bilmasdan turib tizimni boshqarishi mumkin. Bu orqali maxfiy fayllar o‘g‘irlanadi yoki zararli dasturlar o‘rnatiladi.

**4) Malware – Qurilmangizni shikastlovchi zararli dastur**

Malware – virus, troyan, spyware kabi zararli dasturlar umumiy nomi. Ular qurilmangizga kirib, fayllarni buzadi, maxfiy ma’lumotlarni o‘g‘irlaydi yoki qurilmangizni boshqarishni jinoyatchilarga beradi.

Kiberxavfsizlik tahdidlari moliyaviy yo‘qotishlar, ma’lumotlarning buzilishi, shaxsiy ma’lumotlarning o‘g‘irlanishi va asosiy xizmatlardagi uzilishlar kabi zararli oqibatlarga olib kelishi mumkin, bu esa shaxslar, korxonalar va tashkilotlarga ta’sir ko‘rsatadi.

Kiber tahdidlar doimiy ravishda rivojlanib, raqamli tizimlar va tarmoqlarning xavfsizligi va yaxlitligini ta’minlashda jiddiy muammolarni keltirib chiqarmoqda. Ma’lumotlar buzilishining oqibatlari yomon bo‘lib, nafaqat kompaniyaning bevosita moliyaviy holatiga, balki uning obro‘siga va mijozlar ishonchiga ham ta’sir qiladi.

**Internetga asoslangan hujumlar**

Internetga asoslangan hujumlar - bu internet orqali yoki web-ga asoslangan ilovalar orqali amalga oshiriladigan kiber hujumlar. Web-ga asoslangan hujumlarning ba’zi keng tarqalgan turlari:

Saytlararo skript (XSS) hujumlari: Bu hujumlar web-sahifaga zararli kodni kiritishni o‘z ichiga oladi, keyin esa foydalanuvchi brauzeri tomonidan amalga oshiriladi. Bu tajovuzkorga maxfiy maʼlumotlarni oʻgʻirlash yoki foydalanuvchi hisobini nazorat qilish imkonini beradi.

SQL in’ektsiya hujumlari: Bu hujumlar zararli SQL kodini kiritish uchun web-ilovalardagi zaifliklardan foydalanadi, bu esa tajovuzkorga ma’lumotlarni o‘g‘irlash yoki dasturni nazorat qilish imkonini beradi.

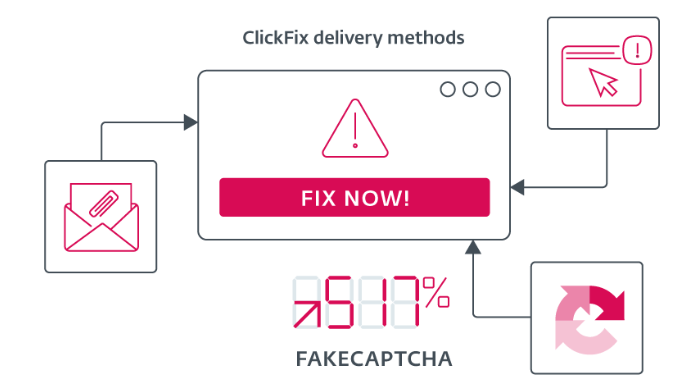
Saytlararo so‘rovlarni qalbakilashtirish (CSRF) hujumlari: Bu hujumlar foydalanuvchini ularning bilimi yoki roziligisiz web-saytdagi harakatni amalga oshirishga undaydi. Bu tajovuzkorga ruxsatsiz xaridlarni amalga oshirish yoki hisob sozlamalarini o‘zgartirish kabi foydalanuvchi nomidan harakatlarni amalga oshirishga ruxsat berishi mumkin.

Seansni o‘g‘irlash hujumlari: Bu hujumlar o‘z hisobiga ruxsatsiz kirish uchun foydalanuvchining seans identifikatorini o‘g‘irlashni o‘z ichiga oladi. Bu tarmoq trafigini tinglash yoki cookie-fayllarni o‘g‘irlash kabi turli vositalar orqali amalga oshirilishi mumkin.

DNS Spoofing - bu kompyuter xavfsizligini buzishning bir turi. Bu orqali ma’lumotlar DNS-resolverning keshiga kiritiladi, bu esa nom serverining noto‘g‘ri IP-manzilni qaytarishiga olib keladi va trafikni tajovuzkorning kompyuteriga yoki boshqa har qanday kompyuterga yo‘naltiradi. DNS spoofing hujumlari uzoq vaqt davomida aniqlanmasdan davom etishi va jiddiy xavfsizlik muammolarini keltirib chiqarishi mumkin.

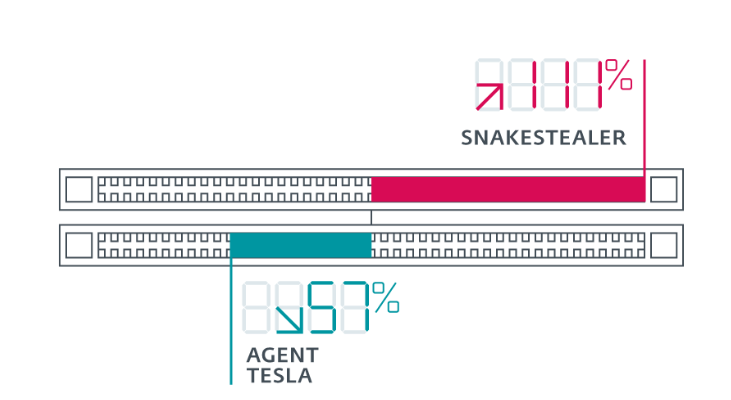
**2.** Hozirgi kunda zamonaviy kiberhujumlardan himoyalanish uchun turli hil himoya dasturlari, antiviruslar, reCaptcha lar ishlatilinmoqda. Ammo shunga mos shaklda kiberhujumlar ham rivojlanib boryapti.  
**ClickFix: Yangi ijtimoiy muhandislik tahdidi**

ESET tomonidan ClickFix/FakeCaptcha  aniqlanishi olti oy ichida **517% ga oshdi** va foydalanuvchilarni soxta xato xabarlari orqali zararli buyruqlarni ishga tushirishga undadi. Endi u bloklangan hujumlarning 8 foizini tashkil etadi va to‘lov dasturi va josuslik dasturlari kabi tahdidlar bilan Windows, Linux va macOS’ni nishonga oladi.



**SnakeStealer Infostealer tojini oladi**

SnakeStealer 2025-yilning birinchi yarmida parollar, tugmalar bosish va skrinshotlarni o‘g‘irlagan holda eng ko‘p aniqlangan ma’lumot o‘g‘irlovchisi sifatida Tesla agentini ortda qoldirdi. 2024-yilning 2-yarmi bilan solishtirganda **+111% ga ikki baravar koʻpaygan** holda , u hozirda maʼlumotlar oʻgʻirlanishini aniqlashning deyarli 20% ni tashkil etadi va bu maʼlumotlar oʻgʻirlanishi qanchalik tez rivojlanayotganini koʻrsatadi.

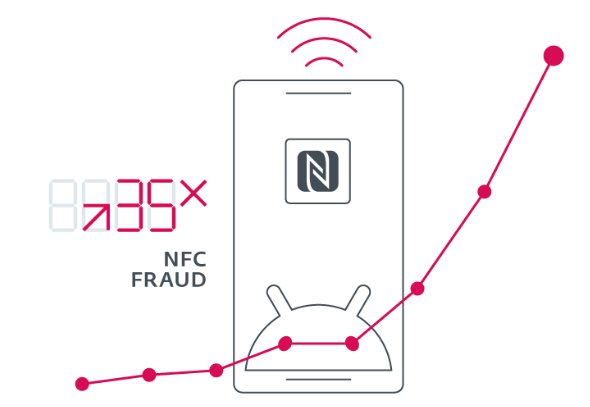


**Axborot o'g'irlovchilariga qarshi kurash**

ESET 2025 yil boshida 21 foizga o'sgan **Lumma Stealer** va AQSh (44 foiz) va Polsha (29 foiz) hujumlari natijasida 52 foizga o'sgan Danabot xizmatlarini buzish uchun global huquqni muhofaza qilish organlariga qo'shildi . Bu muvofiqlashtirilgan harakatlar kuchayib borayotgan tahdidlarga katta zarba berdi.

**Android NFC firibgarligi portladi**

**NFC firibgarligi** 2024 yilning 2-yarmidan boshlab yangi zararli dasturlar variantlari va relayli firibgarliklar tufayli o'ttiz besh baravar oshdi. **NGate** bankomatdan soxta pul yechib olish uchun buzilgan telefonlar orqali toʻlov kartalaridan NFC maʼlumotlarini uzatadi, **GhostTap** esa kontaktsiz toʻlovlar uchun raqamli hamyonlarga yuklash uchun karta maʼlumotlarini oʻgʻirlaydi. O'zini NFC bilan bog'liq zararsiz ilova sifatida ko'rsatadigan SuperCard X tez to'lovlar uchun karta ma'lumotlarini jimgina yozib oladi va uzatadi.



**Kaleydoskop: yangi reklama dasturi**

2025-yilning birinchi yarmida Android reklama dasturlarini **aniqlash 160% ga oshdi , Kaleydoskop deb nomlangan yangi tahdid esa 28% ni tashkil etdi** . U norasmiy ilovalarga tayanadigan hududlarga eng koʻp taʼsir qilib, zararli dasturlarni tarqatish uchun “yovuz egizak” hiylasidan foydalanadi.

**3. Kengash bo'ylab kiber jinoyatlar narxining oshishi.**

Infografika [Accenture](https://www.accenture.com/us-en/insights/security/cost-cybercrime-study) kompaniyasining "Kiberjinoyat narxi" tadqiqoti ma'lumotlariga qaratilgan bo'lib, unda kibertahdidlar tez sur'atda raqamli landshaftda qanday rivojlanayotgani haqida batafsil ma'lumot berilgan.

Umuman olganda, barcha turdagi kiberhujumlar uchun tashkilotlarning o'rtacha yillik xarajatlari ortib bormoqda. Masalan, 2018-yilda bitta zararli dastur hujumi 2,6 million dollardan ko‘proqqa tushdi, 2017–2018 yillar oralig‘ida to‘lov dasturlari narxi eng ko‘p ko‘tarildi, ya’ni 533 000 dollardan 646 000 dollargacha (21 foizga o‘sish).

Hujumlar turidan qat'i nazar, ma'lumotlarning yo'qolishi va biznesning to'xtatilishi asosiy xarajat omillari ekanligi aniqlandi:

* Zararli dasturiy ta'minot  
  Asosiy oqibati: Axborotni yo'qotish  
  O'rtacha xarajat: $1,4 mln (jami yo'qotishlarning 54%)
* Veb-ga asoslangan hujumlar  
  Asosiy oqibat: Axborotni yo'qotish  
  O'rtacha xarajat: $1,4 million (jami yo'qotishlarning 61%)
* Xizmat ko‘rsatishdan bosh tortish (DOS)  
  Asosiy oqibat: Biznesning uzilishi  
  O‘rtacha xarajat: $1,1 million (jami yo‘qotishlarning 65%)
* Zararli insayderlar  
  Asosiy oqibatlar: Biznesning buzilishi va ma'lumotlarning yo'qolishi  
  O'rtacha xarajat: 1,2 million dollar (har biri 0,6 million dollar, jami yo'qotishlarning 75 foizi)

2018-yilda axborot yo‘qotilishi va biznesdagi uzilishlar umumiy biznes yo‘qotishlarining 75% dan ortig‘ini kiberjinoyatlardan tashkil etdi.

Kiberjinoyat keng tarmoqqa olib keladi

Hech bir soha kiberjinoyatning o'sib borayotgan narxiga ta'sir qilmaydi - hisobotda ta'kidlanishicha, tashkilotlar faqat so'nggi besh yil ichida xavfsizlikni buzish 67 foizga o'sgan. Bank ishi eng koʻp zarar koʻrmoqda, yillik xarajatlar 2018-yilda 18 million dollardan oshib ketdi. [Moliyaviy sabablar](https://www.visualcapitalist.com/hackers-hack-motives-behind-cyberattacks/) doimiy ravishda xakerlar uchun katta ragʻbat boʻlishini hisobga olsak, bu ajablanarli emas .

Mana 15 ta turli sohalarda kiberhujumlarning oʻrtacha narxi (har bir tashkilot uchun, 2017 va 2018 chi yillar):



Qizig'i shundaki, hayot fanlari kompaniyalariga ta'siri bir yil ichida eng ko'p o'sdi (har bir tashkilot uchun 86% ga 10,9 million dollarni tashkil etdi), ikkinchi o'rinda sayohat sanoati (har bir tashkilot uchun 77 foizga 8,2 million dollarni tashkil etdi). Bu, ehtimol, klinik sinov tafsilotlari yoki kredit karta ma'lumotlari kabi onlayn almashiladigan nozik va qimmatli ma'lumotlarning ko'payishi bilan bog'liq.

Accenture kiberjinoyatchilikni yumshatishga yordam beradigan to‘qqizta ilg‘or texnologiyani tahlil qildi va ularning sof tejamkorligini hisoblab chiqdi: jami potentsial tejamkorlikdan har bir texnologiya yoki vosita turiga talab qilinadigan investitsiyalarni hisobga olmaganda.

Deyarli 2,3 million dollarlik sof jamg'arma bilan ko'plab kompaniyalar xavfsizlik ma'lumotlari bilan birga keladigan yuqori daromadni tan olishadi. Boshqa tomondan, avtomatlashtirish, sun'iy intellekt va mashinani o'rganishdan foydalanish 2 million dollardan ko'proq mablag'ni tejashga yordam beradi, ammo hozirgacha korxonalarning atigi 38 foizi ushbu yechimni qo'llagan.

Kiberjinoyat kelgusi yillar davomida [keng ko'lamli tashvish](https://www.visualcapitalist.com/cybersecurity-fighting-450b-damage/) bo'lib qoladi. 2019–2023-yillarda global qiymatdagi taxminan 5,2 trillion dollar kiberhujumlar xavfi ostida qoladi va bu korporatsiyalar va investorlar uchun doimiy muammo tug‘diradi.

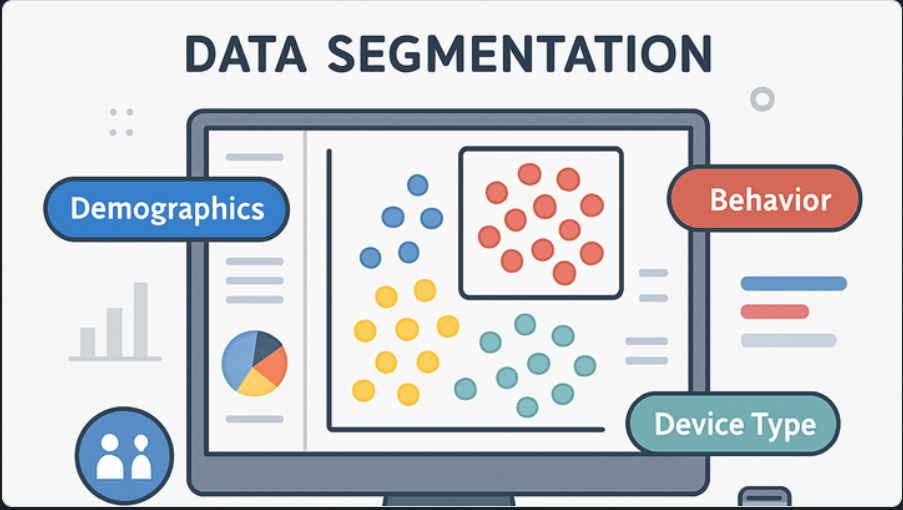
Xuddi shunday xozirgi zamonda internet tarmoqlari, turli hil saytlardan bo’ladigan bir qancha hujumlarni oldini olish uchun insoniyat har xil usullardan foydalanib kelmoqda. Bular: Firewallar, antiviruslar, reCaptchalar, lekin ularning rivojlanishi kiberhujumlarni ham rivojlantiryapti. Hozirgi kunda esa tarmoqdagi malumotlarni bo’lish yani **segmentatsiya** qilish eng yaxshi usullardan biri sifatida qo’llanilyapti.

**4.** **Axborotni ajratish (segmentation) tushunchasi.**

Ma'lumotlarni segmentatsiyalash - bu sizning ma'lumotlaringizni kamida ikkita kichik to'plamga guruhlash jarayonidir, ammo nozik ma'lumotlarga ega bo'lgan katta tarmoqda ko'proq ajratish kerak bo'lishi mumkin. Ma'lumotlar foydalanish holatlari va ma'lumotlar turlari bo'yicha, shuningdek, ushbu ma'lumotlarning sezgirligi va ushbu turdagi ma'lumotlarga kirish uchun zarur bo'lgan vakolat darajasiga qarab guruhlanishi kerak. Ma'lumotlar segmentlangandan so'ng, mavjud ma'lumotlar segmentiga qarab turli xil xavfsizlik parametrlari va autentifikatsiya qoidalari o'rnatilishi kerak.

Agar xaker tarmoqning an'anaviy perimetri xavfsizlik devoridan o'tib ketsa va u tarmoq ma'lumotlarni segmentatsiyalash jarayonini o'tkazib yuborsa, endi xaker segmentdagi ma'lumotlarning kichik bir qismiga emas, balki hamma narsaga kirish huquqiga ega. Ma'lumotlar segmentatsiyasining yo'qligi ko'proq ma'lumotlarni xavfsizlik buzilishiga qarshi himoyasiz qoldiradi, shuningdek, kengroq tarmoq landshaftida buzilish manbasini topish va to'xtatishni qiyinlashtiradi.

Shunday qilib, ma'lumotlarni segmentatsiyalash g'oyasi ma'lumotlaringizni toifalarga bo'lish, eng nozik ma'lumotlarni qolganlaridan ajratish va ularni himoya sirtingiz sifatida belgilash va keyin siz aniqlagan har qanday himoya sirtlari atrofida qo'shimcha xavfsizlik choralarini qo'llashdir. Agar buzilish sodir bo'lsa ham, sizning eng nozik ma'lumotlaringiz endi qo'shimcha xavfsizlik choralari bilan himoyalangan.



**5.Tarmoq segmentatsiyasi va uning turlari**

Band bo'lgan aeroport terminali orqali navigatsiya tarmoq segmentatsiyasidan unchalik farq qilmaydi. Aeroportdan o'tish bir nechta xavfsizlik nazorat punktlarini tozalashni o'z ichiga oladi, shu bilan birga oxir-oqibat manzilingizga etib borishdan oldin cheksiz darvozalar orasida o'z yo'lingizni topasiz.

Ko'p kirish boshqaruvlari har bir nuqtadan tashqarida ruxsatsiz kirishni cheklaydi, va segmentlangan zonalarga mantiqiy tashkilot - chiptalar, konkurslar, darvozalar - yo'lovchilar tartibsizliklarga qaramay intuitiv ravishda harakat qilishlari uchun tuzilmani yaratadi. Tarmoq segmentatsiyasi xuddi shunday tarzda ishlaydi, xavfsizlik, monitoring va kirishni boshqarishni yaxshilash uchun tarmoqlarni qismlarga ajratilgan zonalarga ajratadi.

Tarmoq segmentatsiyasi - bu kattaroq kompyuter tarmog'ini bir nechta kichik kichik tarmoqlarga yoki "segmentlarga" bo'lish jarayoni. Ushbu segmentatsiya turli foydalanuvchilarni, qurilmalarni, ilovalarni yoki trafik oqimlarini ajratib turadigan diskret zonalarni yaratadi.Segmentatsiya jismoniy yoki mantiqiy ravishda sodir bo'lishi mumkin.

**Fizik(Jismoniy) tarmoq segmentatsiyasi**

Jismoniy segmentatsiya tarmoqni alohida infratuzilma komponentlariga jismoniy ajratish uchun marshrutizatorlar, kalitlar va xavfsizlik devorlari kabi haqiqiy tarmoq uskunasidan foydalanishni o'z ichiga oladi. Masalan, tashkilot muhandislik quyi tarmog'i, buxgalteriya quyi tarmog'i, mehmon Wi-Fi pastki tarmog'i va boshqalar uchun maxsus marshrutizatorlar va kalitlarni ajratishi mumkin.

Ushbu yondashuv tarmoq trafik oqimlarini to'g'ridan-to'g'ri asosiy uskuna orqali ajratadi. Biroq, jismoniy segmentatsiya har bir zona uchun qimmat yangi uskunalarni sotib olish va sozlashni talab qiladi. Bundan tashqari, agar tashkiliy ehtiyojlar o'zgarsa, unda moslashuvchanlik yo'q.

**Mantiqiy tarmoq segmentatsiyasi**

Mantiqiy segmentatsiya apparat o'rniga tarmoqlarni ajratish uchun virtual tarmoq usullaridan foydalanadi. Ikkita keng tarqalgan misol VLAN va Layer 3 IP-manzil sxemalari:

[VLAN (virtual mahalliy tarmoqlar)](https://www.auvik.com/franklyit/blog/what-is-a-vlan/) hatto bir xil jismoniy kalitda ham kommutator portlarini alohida trafik guruhlariga sozlaydi. Bitta kalitda ulangan qurilmalarni mantiqiy pastki tarmoqlarga bo'lish uchun bir nechta VLAN bo'lishi mumkin.

[3-qatlam](https://www.auvik.com/franklyit/blog/layer-3-switches-layer-2/) tarmoq segmentatsiyasi turli mantiqiy pastki tarmoqlarda qurilmalarning IP manzillarini tayinlaydi. Tarmoqlararo trafik faqat trafikni to'g'ri belgilangan pastki tarmoqqa yo'naltirish orqali ajratishni ta'minlaydigan marshrutizator orqali o'tishi kerak.

Mantiqiy segmentatsiya yangi jihozlarni talab qilmaydi, chunki u mavjud infratuzilmadan foydalanadi. U moslashuvchan, tejamkor va tashkilot rivojlanayotganda qayta konfiguratsiya qilish oson.

**Tarmoq segmentatsiyasi va mikrosegmentatsiya**

Tarmoq segmentatsiyasi va mikrosegmentatsiyasi bir-biriga o'xshash, chunki ular ikkalasi ham tarmoq xavfsizligini oshiradi, lekin ular yondashuv qanchalik batafsil ekanligi bilan farqlanadi.

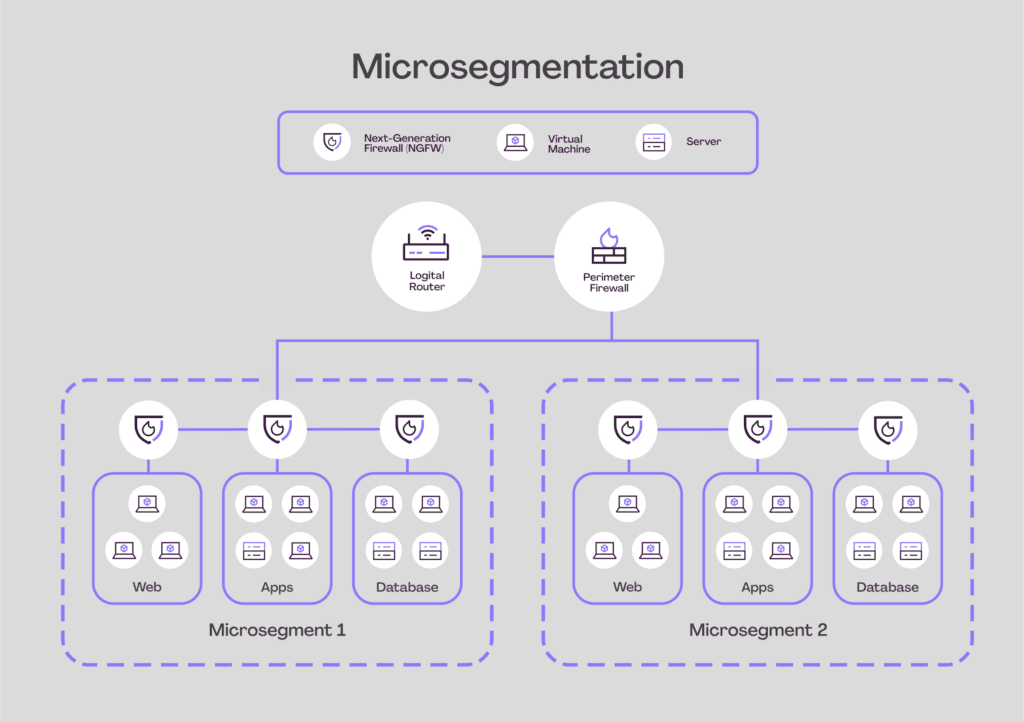
*Tarmoq segmentatsiyasi*

Yuqorida aytib o'tilganidek, tarmoq segmentatsiyasi tarmoqni yuqori darajada katta mantiqiy yoki jismoniy kichik tarmoqlarga ajratadi. Masalan, tarmoq segmentatsiyasi turli biznes birliklari, funktsiyalari yoki trafik turlarini alohida xavfsizlik zonalariga ajratishi mumkin.

Ushbu tarmoq segmentlari o'zlarining marshrutizatorlari, kalitlari, xavfsizlik devorlari va xavfsizlikni boshqarish vositalariga ega. Biroq, segmentlarning o'zlari hali ham bitta ishonchli domenga guruhlangan ko'plab foydalanuvchilar, qurilmalar va ilovalarni o'z ichiga olgan juda katta muhit bo'lishi mumkin.

*Mikrosegmentatsiya*

Mikrosegmentatsiya tarmoqni bo'linish jarayonini ancha nozik darajaga tushiradi - tarmoqni katta guruhlarga emas, balki juda kichik, individual ish yuklariga bo'linadi. Agar tarmoq segmentatsiyasi butun bo'lim yoki dastur darajasini himoya qilishi mumkin bo'lsa, mikrosegmentatsiya har bir komponentni alohida-alohida bloklaydi, masalan, bitta virtual mashina, konteyner, server, qurilma yoki pod.



Bu aniq tarmoq xavfsizlik devori qoidalari, rolga asoslangan kirishni boshqarish va dastur qatlamini himoya qilish kabi muayyan ish yuklariga sozlangan juda maqsadli xavfsizlik siyosatlarini beradi. Biroq, bu miqyosda xavfsizlikni boshqarish eksponent ravishda murakkabroq.

**Nima uchun tarmoq segmentatsiyasi kerak ?**

Raqamli aktivlaringizni himoya qilish eng muhim vazifadir va xavfsizlik devorlari juda qattiq va belgilangan xavfsizlik devori qoidalariga rioya qilishga qodir bo'lsa-da, ular raqamli aktivlaringizni himoya qilish uchun kerak bo'lgan hamma narsaga erisha olmaydi. Ular, shuningdek, eskirgan bo'lishi mumkin va faqat oldingi mudofaa taklif.

Raqamli innovatsiyalar yangi xizmatlar va tarmoq muhitlarini taqdim etar ekan, xavflar ortadi. Hujumlar an'anaviy tarmoq chegaralaridan tashqarida sodir bo'lishi mumkin. Sizning xavfsizligingiz aqlli yoritish tizimingiz kabi biror narsa orqali buzilgan bo'lsa-da, tahdid tekis tarmoqqa kirish huquqiga ega bo'lgach, maxfiy ma'lumotlarga kirishi mumkin. Biroq, tarmoq segmentatsiyasi boshqa ma'lumotlarga kirish xavfini kamaytiradi.

**6.Segmentatsiya samaradorligi va afzalliklari.**

Uy tarmog'ini yoki biznes uchun kichik tarmoqni o'rnatasizmi, xavfsizlik va trafik haqida o'ylashingiz kerak. Ushbu ikkala muammoni hal qilishning usullaridan biri tarmoq segmentatsiyasidir. Tarmoqni segmentlarga bo'lish orqali siz tarmoqning ishonchliligi va samaradorligini oshirib, xavfsizlik tahdidlariga ta'sir qilishni cheklaysiz.

Tarmoq segmentatsiyasining asosiy amalga oshirilishi yoki tarmoq "segmentlari" ni yaratish, kompyuterlarning alohida klasterlarini tarmoqning qolgan qismidan ajratish uchun markazlar, marshrutizatorlar va ehtimol xavfsizlik devori kabi xavfsizlik dasturlarini qo'llashni o'z ichiga oladi. Shunday qilib, siz qo'shni bo'lmagan tarmoq yaratasiz. Bu shuni anglatadiki, barcha kompyuterlar umumiy Internet protokoli manzili orqali hech qanday farqlashsiz Internetga kirish imkoniga ega bo'lgan odatiy tarmoqdan farqli o'laroq, segmentlar umumiy Internet manbasiga ega bo'lsa ham, tarmoq ichidagi alohida ob'ektlar sifatida ajratilgan.

**Samaradorlik**

Tarmoqni segmentlashning afzalliklaridan biri bu trafik samaradorligi. Kompyuterlar bir-biri bilan aloqa qilganda, ular "paketlar" deb ataladigan ma'lumotlarning bitlarini, shuningdek, aloqa mazmunini, shuningdek jo'natuvchi va qabul qiluvchi haqidagi ma'lumotlarni yuboradilar. Agar ikkita kompyuter bir vaqtning o'zida bir-biriga ma'lumot yuborsa -- yoki bir nechta kompyuterlar bir-biriga ma'lumot yuborsa - "paket to'qnashuvi" sodir bo'lishi mumkin, bu yuborilgan ma'lumotni buzadi va aloqani buzadi. Katta qismlarga ajratilmagan tarmoqlar bilan ishlashda barcha kompyuterlar boshqa barcha kompyuterlar bilan bog'lana oladi va to'qnashuv ehtimoli paydo bo'ladi. Segmentlangan tarmoq yordamida kompyuterlar ko'p hollarda segmentlar ichida aloqa o'rnatishi mumkin, bu esa umumiy tarmoqdagi trafik hajmini kamaytiradi va paketlar to'qnashuvi ehtimolini kamaytiradi.

**7. Xulosa**

Tarmoqni segmentlarga ajratish ham aloqa samaradorligini oshirish imkonini beradi. Paket to'qnashuvi bilan bir qatorda, segmentlanmagan tarmoqdagi kompyuterlarning katta hajmi tarmoqning o'tkazish qobiliyatidan foydalanishni oshiradi. Agar tarmoqda veb-sahifalarni ta'minlovchi serverlar mavjud bo'lsa, siz kiruvchi trafikni segmentlar o'rtasida "muvozanatli" bo'lishini belgilashingiz mumkin, shunda hech bir alohida segment yoki tarmoq barcha kiruvchi yoki chiquvchi trafik bilan shug'ullanmasligi kerak. Bu shuni anglatadiki, sizning tarmog'ingiz umumiy hajmdagi trafikni boshqara oladi, shuningdek, keyinchalik kengaytirishga yaxshiroq tayyor bo'ling.

Segmentatsiya sizga bir qator xavfsizlik imtiyozlarini beradi. Birinchisi, trafikni taqsimlamaydigan segmentlarga ega bo'lishdan kelib chiqadi, ya'ni agar kompyuter bir segmentda buzilgan bo'lsa, u avtomatik ravishda tajovuzkorga boshqa segmentdagi kompyuterlarga kirish huquqini bermaydi. Bu tahdid ta'sirini cheklaydi. Ikkinchidan, siz har bir segmentni xavfsizlik dasturlari va xavfsizlik devorlari orqali har xil tarzda himoya qilishingiz mumkin, shunda tajovuzkor turli segmentlarga kirish uchun turli xavfsizlik to'plamlarini buzishi kerak, bu esa butun tizimni buzishni qiyinlashtiradi.

**Tarmoq segmentatsiyasi** zamonaviy AT xavfsizligi strategiyalarining markaziy elementidir. U kompaniyalarni hujumlarning nazoratsiz tarqalishidan himoya qiladi, ish faoliyatini yaxshilaydi va me'yoriy hujjatlarga rioya qilishni qo'llab-quvvatlaydi. Ayniqsa, kiber tahdidlar kuchayib borayotgan davrda segmentatsiya endi tanlov emas, balki majburiydir. Docusnap kabi yechim bilan kompaniyalar nafaqat o'z tarmoqlarini shaffof tarzda taqdim etishlari, balki segmentatsiya tadbirlarini samarali rejalashtirishlari, hujjatlashtirishlari va nazorat qilishlari mumkin. Bu xodimlarning mehnat unumdorligini cheklamasdan, xavfsizlikni barqaror mustahkamlaydi.

**8.Foydalanilgan adabiyotlar va saytlar ro’yhati:**

1. Cybersecurity Threats, Malware Trends, and Strategies — Tim Rains (2023).

2. Information Technology Security: Modern Trends and Challenges — Springer (2024).

3. Cyber Security 2025 Trends — Mark Hayward (2025).

4. NIST — Data classification / data-centric security management (NCCoE / SP-1800 shablon va IR).

5. OWASP — Network Segmentation Cheat Sheet (segmentatsiya tamoyillari).

6. ESET Threat Report H1 2025.

7. Red Canary Threat Detection Report.

8. Building stronger defences for a digital future: The role of cybersecurity: Economic Security in a Changing World.

9. CISA “Layering Network Security Through Segmentation”.

10. Fortinet – “What Is Network Segmentation?”.

11. DiverseDaily – “Network Segmentation: Benefits and Implementation of Network Segmentation”.