TARMOQDA AXBOROTNI HIMOYA QILISH.VPN (VIRTUAL PRIVATE NETWORK) VIRTUAL XUSUSIY TARMOQ.

Ilmiy rahbar: Rahmonov Mirzohidjon Shavkatovich. *Andijon davlat pedagogika instituti Aniq fanlar fakulteti Matematika va informatika kafedrasi dotsenti*

Mamasoliyeva Muharramxon Abdujalil qizi *Andijon davlat pedagogika instituti Aniq fanlar fakulteti Matematika va informatika yo'nalishi 3-bosqich talabasi*

Annotatsiya: Axborotni himoya qilish zamonaviy kompyuter tizimlarida va tarmoqlarida uzatilayotgan, saqlanayotgan va qayta ishlanayotgan axborotning ishonchliligini va butunligini tizimli ta'minlash maqsadida turli xil vositalarni va usullarni ishlatish, choralarni ko'rish va VPN (Virtual Private Network) virtual xususiy tarmoq. Bu texnologiya foydalanuvchilar o'rtasida barcha ma'lumotlarni almashish boshqa tarmoq doirasida ichki tarmoqni shakllantirishga asoslangan, ishonchli himoyani ta'minlashga qaratilgan. VPN uchun tarmoq asosi sifatida Internetdan foydalanish aytib o'tilgan.kazish tushuniladi.

Kalit so'zlar: Axborotni himoya qilish, global tarmoq, axborotni uzatish, axborot xavfsizligi bo'yicha yo'l qo'yiladigan keng tarqalgan to'qqizta xatolar, WWW, FTP, Gophes serverlar, VPN texnologiyasi, VPN ishlash tamoyili.

Kirish: Bugungi kunda axborot texnologiyalari sohasi respublikamizning rivojlanishida muhim o'rin tutib kelmoqda. O'tgan yillar mobaynida O'zbekiston Respublikasi hukumati tomonidan axborot kommunikatsiya texnologiyalarini keng joriy qilish va rivojlantirish borasida olib borgan siyosati hozirgi kunga kelib o'z natijalarini ko'rsatmoqda. Har bir soha faoliyatida kompyuter texnologiyalari va internet tarmog'idan foydalanish ish unumdorligini oshirmoqda. Bizga ma'lumki hayotiy faoliyatimizda ahamiyatli ro'liga ega bo'lgan har qanday yo'nalish borki unga nisbatan tahdidlar, xato va kamchiliklar va albatta o'ziga xos yutuqlardan tashkil topadi. Sohalardagi AKTga talab ortib borgani sari uni himoyalashga, tahdidlarni oldini olishga bo'lgan talab keskin ortdi. Ushbu talablarni amalga oshirish uchun innovatsion usullarini izlab topish, axborotlashtirish jarayoniga har tomonlama ko'maklashish, ularni hayotga keng joriy etish, xavfsizligini himoya qilishda apparat va dasturiy maxsulotlardan samarali foydalanish sohalar faoliyatining muhim yo'nalishlaridan biriga aylanmoqda. Zero, axborotlashtirish tizimida davlat siyosatini olib borish masalasi strategik ahamiyatga ega vazifadir.

Umumiy axborot kengligining yaratilishi va shaxsiy kompyuterlarning amaliy jihatdan keng qo‘llanilishi va kompyuter tizimlari va tarmoqlarining tatbiq etilishi axborotni himoya qilish muammosini yechish zarurligini keltirib chiqaradi.

Axborotni himoya qilish deganda zamonaviy kompyuter tizimlarida va tarmoqlarida uzatilayotgan, saqlanayotgan va qayta ishlanayotgan axborotning ishonchliligini va butunligini tizimli ta‘minlash maqsadida turli xil vositalarni va usullarni ishlatish, choralarni ko‘rish va tadbirlarni o‘t

Axborotni himoya qilish - bu:

- axborotning fizik butunligini ta‘minlash, ya‘ni axborot elementlarini to‘siqlarga uchrashiga va yo‘qolishiga yo‘l qo‘ymaslik;
- axborot butunligini saqlashda uning elementlarini almashtirishga (modifikasiyaga) yo‘l qo‘ymaslik;
- mos vakolatlarga ega bo‘lmagan shaxslar yoki jarayonlar tomonidan taqiqlangan axborotni olinishiga yo‘l qo‘ymaslik;
- egalariga uzatilayotgan resurslar faqatgina tomonlar kelishgan shartlarga mos ravishda ishlatilishiga ishonch hosil qilinishi kerak.

Global tarmoqlarning rivojlanishi va axborotlarni olish, qayta ishlash va uzatishning yangi texnologiyalari paydo bo‘lishi bilan Internet tarmog‘iga har xil shaxs va tashkilotlarning e‘tibori qaratildi. Ko‘plab tashkilotlar o‘z lokal tarmoqlarini global tarmoqlarga ulashga qaror qilishgan va hozirgi paytda WWW, FTP, Gophes va boshqa serverlardan foydalanishmoqda. Tijorat maqsadida ishlatiluvchi yoki davlat siri bo‘lgan axborotlarning global tarmoqlar bo‘yicha joylarga uzatish imkoni paydo bo‘ldi va o‘z navbatida, shu axborotlarni himoyalash tizimida malakali mutaxassislarga ehtiyoj tug‘ilmoq. Global tarmoqlardan foydalanish bu faqatgina «qiziqarli» axborotlarni izlash emas, balki tijorat maqsadida va boshqa ahamiyatga molik ishlarni bajarishdan iborat. Bunday faoliyat vaqtida axborotlarni himoyalash vositalarining yo‘qligi tufayli ko‘plab talofotlarga duch kelish mumkin.

Aynan tarmoqdan foydalangan holda tezkor ma‘lumot almashish vaqtdan yutish imkonini beradi. Xususan, yurtimizda Elektron hukumat tizimi shakllantirilishi va uning zamirida davlat boshqaruv organlari hamda aholi o‘rtasidagi o‘zaro aloqaning mustahkamlanishini tashkil etish tarmoqdan foydalangan holda amalga oshadi. Tarmoqdan samarali foydalanish demokratik axborotlashgan jamiyatni shakllantirishni ta‘minlaydi. Bunday jamiyatda, axborot almashinuv tezligi yuksaladi, axborotlarni yig‘ish, saqlash, qayta ishlash va ulardan foydalanish bo‘yicha tezkor natijaga ega bo‘linadi.

Biroq tarmoqqa noqonuniy kirish, axborotlardan foydalanish va o‘zgartirish, yo‘qotish kabi muammolardan himoya qilish dolzarb masala bo‘lib qoldi. Ish faoliyatini tarmoq bilan bog‘lagan korxona, tashkilotlar hamda davlat idoralari ma‘lumot almashish

uchun tarmoqqa bog‘lanishidan oldin tarmoq xavfsizligiga jiddiy e‘tibor qaratishi kerak. Tarmoq xavfsizligi uzatilayotgan, saqlanayotgan va qayta ishlanayotgan axborotni ishonchli tizimli tarzda ta‘minlash maqsadida turli vositalar va usullarni qo‘llash, choralarni ko‘rish va tadbirlarni amalga oshirish orqali amalga oshiriladi. Tarmoq xavsizligini ta‘minlash maqsadida qo‘llanilgan vosita xavf-xatarni tezda aniqlashi va unga nisbatan qarshi chora ko‘rishi kerak. Tarmoq xavfsizligiga tahdidlarning ko‘p turlari bor, biroq ular bir necha toifalarga bo‘linadi:

- axborotni uzatish jarayonida hujum qilish orqali, eshitish va o‘zgartirish (Eavesdropping);
- xizmat ko‘rsatishdan voz kechish; (Denial-of-service)
- portlarni tekshirish (Port scanning).

Axborotni uzatish jarayonida, eshitish va o‘zgartirish hujumi bilan telefon aloqa liniyalari, internet orqali tezkor xabar almashish, videokonferensiya va faks jo‘natmalari orqali amalga oshiriladigan axborot almashinuvida foyda-lanuvchilarga sezdirmagan holatda axborotlarni tinglash, o‘zgartirish hamda to‘sib qo‘yish mumkin. Bir qancha tarmoqni tahlillovchi protokollar orqali bu hujumni amalga oshirish mumkin. Hujumni amalga oshiruvchi dasturiy ta‘minotlar orqali CODEC (video yoki ovozli analog signalni raqamli signalga aylantirib berish va aksincha) standartidagi raqamli tovushni osonlik bilan yuqori sifatli, ammo katta hajmni egallaydigan ovozli fayllar (WAV)ga aylantirib beradi. Odatda bu hujumning amalga oshirilish jarayoni foydalanuvchiga umuman sezilmaydi. Tizim ortiqcha zo‘riqishlarsiz va shovqinsiz belgilangan amallarni bajaraveradi. Axborotning o‘g‘irlanishi haqida mutlaqo shubha tug‘ilmaydi. Faqatgina oldindan ushbu tahdid haqida ma‘lumotga ega bo‘lgan va yuborilayotgan axborotning o‘z qiymatini saqlab qolishini xohlovchilar maxsus tarmoq xafvsizlik choralarini qo‘llash natijasida himoyalangan tarmoq orqali ma‘lumot almashish imkoniyatiga ega bo‘ladilar.

Axborot xavfsizligi bo‘yicha yo‘l qo‘yiladigan keng tarqalgan to’qqizta xatolar:

Stikerlarda parollar;

1. Kompyuterni ishlash paytida qarovsiz qoldirish;
2. Begona kompyuterlarda electron pochta ilovalarini ochish;
3. Parolning yomon tuzilishi (hayvonlar, avtomobillar nomlari, ismlar);
4. Portativ kompyuterlardan erkin foydalanish;
5. Mahmadonalik;
6. Ishga solish va o‘ynash;
7. Qayd etilmagan xavfsizlikni buzish;
8. Xavfsizlik tizimi bo‘yicha yangilanishlarni o‘rnatishni doim keyinga qoldirish;
9. Tashkilot ichidagi xavflarga e‘tiborsizlik.

Tarmoq orqali ma‘lumot almashish mobaynida yuborilayotgan axborotni eshitish va o‘zgartirishga qarshi bir necha samarali natija beruvchi texnologiyalar mavjud:

- IPSec (Internet protocol security) protokoli;
- VPN (Virtual Private Network) virtual xususiy tarmoq;
- IDS (Intrusion Detection System) ruhsatsiz kirishlarni aniqlash tizimi.

VPN (Virtual Private Network) virtual xususiy tarmoq sifatida ta‘riflanadi. Bu texnologiya foydalanuvchilar o‘rtasida barcha ma‘lumotlarni almashish boshqa tarmoq doirasida ichki tarmoqni shakllantirishga asoslangan, ishonchli himoyani ta‘minlashga qaratilgan. VPN uchun tarmoq asosi sifatida Internetdan foydalaniladi.

VPN texnologiyasining afzalligi. Lokal tarmoqlarni umumiy VPN tarmog‘iga birlashtirish orqali kam xarajatli va yuqori darajali himoyalangan tunelni qurish mumkin. Bunday tarmoqni yaratish uchun sizga har bir tarmoq qismining bitta kompyuteriga filiallar o‘rtasida ma‘lumot almashishiga xizmat qiluvchi maxsus VPN shlyuz o‘rnatish kerak. Har bir bo‘limda axborot almashishi oddiy usulda amalga oshiriladi. Agar VPN tarmog‘ining boshqa qismiga ma‘lumot jo‘natish kerak bo‘lsa, bu holda barcha ma‘lumotlar shlyuzga jo‘natiladi. O‘z navbatida, shlyuz ma‘lumotlarni qayta ishlashni amalga oshiradi, ishonchli algoritm asosida shifrlaydi va Internet tarmog‘i orqali boshqa filialdagi shlyuzga jo‘natadi. Belgilangan nuqtada ma‘lumotlar qayta deshifrlanadi va oxirgi kompyuterga oddiy usulda uzatiladi. Bularning barchasi foydalanuvchi uchun umuman sezilmas darajada amalga oshadi hamda lokal tarmoqda ishlashdan hech qanday farq qilmaydi. Eavesdropping hujumidan foydalanib, tinglangan axborot tushunarsiz bo‘ladi.

Bundan tashqari, VPN alohida kompyuterni tashkilotning lokal tarmog‘iga qo‘shishning ajoyib usuli hisoblanadi. Tasavvur qilamiz, xizmat safariga noutbukingiz bilan chiqqansiz, o‘z tarmog‘ingizga ulanish yoki u yyerdan biror-bir ma‘lumotni olish zaruriyati paydo bo‘ldi. Maxsus dastur yordamida VPN shlyuz bilan bog‘lanishingiz mumkin va ofisda joylashgan har bir ishchi kabi faoliyat olib borishigiz mumkin. Bu nafaqat qulay, balki arzondir.

VPN ishlash tamoyili. VPN tarmog‘ini tashkil etish uchun yangi qurilmalar va dasturiy ta‘minotdan tashqari ikkita asosiy qismga ham ega bo‘lish lozim: ma‘lumot uzatish protokoli va uning himoyasi bo‘yicha vositalar.

Ruhsatsiz kirishni aniqlash tizimi (IDS) yordamida tizim yoki tarmoq xavfsizlik siyosatini buzib kirishga harakat qilingan usul yoki vositalar aniqlanadi. Ruhsatsiz kirishlarni aniqlash tizimlari deyarli chorak asrlik tarixga ega. Ruhsatsiz kirishlarni aniqlash tizimlarining ilk modellari va prototiplari kompyuter tizimlarining audit ma‘lumotlarini tahlillashdan foydalangan. Bu tizim ikkita

asosiy sinfga ajratiladi. Tarmoqqa ruhsatsiz kirishni aniqlash tizimi (Network Intrusion Detection System) va kompyuterga ruhsatsiz kirishni aniqlash tizimiga (Host Intrusion Detection System) bo‘linadi.

Foydalanilgan adabiyotlar:

1. Andrew S. Tanenbaum, Computer Networks, 5th Edition, Prentice Hall, 2010.
2. Larry L. Peterson and Bruce S. Davie, Computer Networks: A Systems Approach, 5th Edition, Morgan Kaufmann, 2012.
3. Behrouz A. Forouzan, Data Communications and Networking, 5th Edition, McGraw-Hill, 2012.
4. James F. Kurose and Keith W. Ross, Computer Networking: A Top-Down Approach, 7th Edition, Pearson, 2017.
5. Douglas E. Comer, Computer Networks and Internets, 6th Edition, Pearson, 2015.
6. Kizza, Jozef Migga. Kompyuter tarmog'ining xavfsizligi bo'yicha qo'llanma. Berlin: Springer, 2017. Chop etish
7. Harrington, Jan L. Tarmoq xavfsizligi: amaliy yondashuv. Kembrij: Akademik matbuot, 2005 yil. Chop etish