KOMPYUTER TARMOG`INING XAVFSIZLIGINI TA`MINLASH

Ilmiy rahbar: **Karimova N.I**
Islom Karimov nomidagi Toshkent davlat texnika universiteti o'qituvchisi
Rahimova Mohira Muzaffar qizi
Islom Karimov nomidagi Toshkent davlat texnika universiteti talabasi
mohira2000@inbox.ru

Annotatsiya: *Axborot xavfsizligini ta'minlash – bu foydalanuvchining axborotlarini himoyalashga quyilgan me'yor va talablarni bajarishidir. Axborot xavfsizligi esa bu axborot foydalanuvchilariga va ko'plab axborot tizimlariga zarar keltiruvchi tabiiy yoki sun'iy xarakterga ega tasodifiy va uyushtirilgan ta'sirlardan axborotlarni va axborot kommunikatsiya tizim ob'ektlarining himoyalanganligidir.*

Kalit so'zlar: *Kompyuter tarmog`i, axborotni himoyalash, login, parol, avtorizatsiya, resurs, virus, hujum.*

Kompyuter tarmog`i- bu ma`lumotlar uzatishning asosiy tarmog`ini tashkil etib telekommunikatsiya vositalardan foydalangan holda yagona tarmoqqa birlashtirgan kompyuterlar to`plami.

Tarmoq xavfsizligini ta'minlash uchun siz Internet-provayder tarmoqlari orqali paket sifatida harakatlanadigan ma'lumotlarni buzishingiz, buzib tashlamasligingiz yoki ruxsatsiz shaxslar tomonidan tutilmasligi uchun himoya qilishingiz kerak. Ushbu muammoni hal qilish uchun bugungi kunda virtual xususiy tarmoqlar (VPN) mexanizmi keng qo'llanilmoqda.

Avtonom ishlaydigan kompyuter tashqi hujumlardan ozmi-ko'pmi samarali himoyalangan bo'lishi mumkin. Bu tarmoq xavfsizligi vositalarining ko'pchiligining diqqat markazida turadi. Tarmoq xavfsizligi muammolari korporativ tarmoqlarning Internetdan transport vositasi sifatida tobora ko'proq foydalanishi tufayli muhim ahamiyat kasb etmoqda.

Xavfsiz axborot tizimini ta'minlash uchun: ma'lumotlarni ruxsatsiz kirishdan himoya qilish; foydalanuvchilaringizga ma'lumot berishga doimo tayyor bo'lish; ma'lumotlarni xavfsiz saqlash va ma'lumotlarning o'zgarmasligini kafolatlash kerak. Buning uchun tizim quyidagi xususiyatlarga ega bo'lishi kerak:

Maxfiylik - bu maxfiy ma'lumotlar faqat vakolatli foydalanuvchilar uchun mavjud bo'lishni kafolati.

Mavjudligi - vakolatli foydalanuvchilar har doim ma'lumotlarga kirish huquqining kafolati.

Butunlik - bu ma'lumotlar xavfsizligining kafolati bo'lib, u ruxsatsiz foydalanuvchilarning har qanday tarzda ma'lumotlarni o'zgartirishi, yo'q qilishi yoki yaratishi taqiqlanishi bilan ta'minlanadi.

Asosiy tarmoq xavfsizligi xizmatlarini ko'rib chiqamiz.

Shifrlash - bu ma’lumotni oddiy "tushunarli" shakldan "tushunarsiz" shifrlangan shaklga o‘zgartiradigan protsedura. Shifrlangan ma’lumotni parolini hal qilish uchun parolni hal qilish protsedurasidan foydalaniladi. Jarayonlar juftligi - shifrlash va parol hal qilish - kriptosistema deb ataladi. Shifrlash foydalanuvchi autentifikatsiyasi yoki avtorizatsiya tizimlarida, shuningdek aloqa kanallari xavfsizligi va ma’lumotlarni saqlash tizimlarida ishlatilishi mumkin.

Autentifikatsiya (yunoncha authetikos - asl, inglizcha autentifikatsiya - identifikatsiya,) - autentifikatsiya - ruxsatsiz shaxslar tomonidan tarmoqqa ruxsatsiz kirishni oldini oladi va qonuniy foydalanuvchilarga kirish imkoniyatini beradi. Faqat foydalanuvchilar autentifikatsiyani talab qiladigan ob’yektlar sifatida emas, balki turli xil ilovalar, qurilmalar va ma’lumotlarni ham bajarishlari mumkin.

Dastur darajasida autentifikatsiyaning misoli - mijoz va serverning o‘zaro autentifikatsiyasi, bu erda serverda qonuniyligini isbotlagan mijoz, shuningdek, dialog 340 haqiqatan ham o‘z serverida ekanligiga ishonch hosil qilishi kerak. Ikkala qurilma o‘rtasida aloqa seansini o‘rnatishda o‘zaro autentifikatsiya protsedurasi ham ta'minlanishi mumkin. Ma’lumotlarni autentifikatsiya qilish ushbu ma’lumotlarning yaxlitligini, shuningdek ularni e'lon qilgan kishidan kelib chiqqanligini isbotlashni anglatadi. Buning uchun elektron imzo mexanizmidan foydalaniladi. Autentifikatsiyani identifikatsiya qilish va avtorizatsiya qilish bilan aralashtirmaslik kerak. Identifikatsiya foydalanuvchida tizimga uning identifikatorini aytib berishidan iborat, autentifikatsiya esa foydalanuvchi o‘zi deb da'vo qilgan shaxs ekanligini isbotlash protsedurasi, xususan o‘zi kiritgan identifikatorga egalik qilishining dalili. Tizimda foydalanuvchi identifikatorlari boshqa ob’yektlarning (fayllar, jarayonlar, ma’lumotlar tuzilmalari) identifikatorlari bilan bir xil maqsadlarda ishlatiladi va ular har doim ham xavfsizlik bilan bevosita bog‘liq emas.

Avtorizatsiya - bu yuridik foydalanuvchilarning tizim resurslaridan foydalanish huquqini boshqarish, ularning har biriga ma'muriyat tomonidan o‘zi uchun aniq belgilab qo‘yilgan huquqlarni berish bilan nazorat qilish tartibi. Avtorizatsiya tizimi foydalanuvchilarga kataloglar, fayllar va printerlarga kirish huquqini berish bilan bir qatorda foydalanuvchilarning turli xil tizim funktsiyalarini bajarishi mumkin, masalan, serverga lokal kirish, tizim vaqtini belgilash, ma’lumotlarning zaxira nusxasini yaratish, serverni o‘chirish va hk.

Audit - himoyalangan tizim resurslariga kirish bilan bog‘liq voqealarni tizim jurnalida qayd etish. Zamonaviy operatsion tizimlarning auditorlik quyi tizimi ma'muriyatni qiziqtirgan voqealar ro‘yxatini qulay grafik interfeys yordamida farqlashga imkon beradi. Buxgalteriya hisobi va monitoring vositalari xavfsizlikning muhim hodisalarini aniqlash va qayd etish imkoniyatini beradi; tizim resurslarini yaratish, kirish yoki o‘chirish uchun har qanday urinishlar (shu jumladan muvaffaqiyatsiz bo‘lganlar).

Kompyuter tarmog‘ining xavfsizlik xizmatlari

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 foydalanuvchilarga 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. 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) ruxsatsiz kirishlarni aniqlash tizimi.

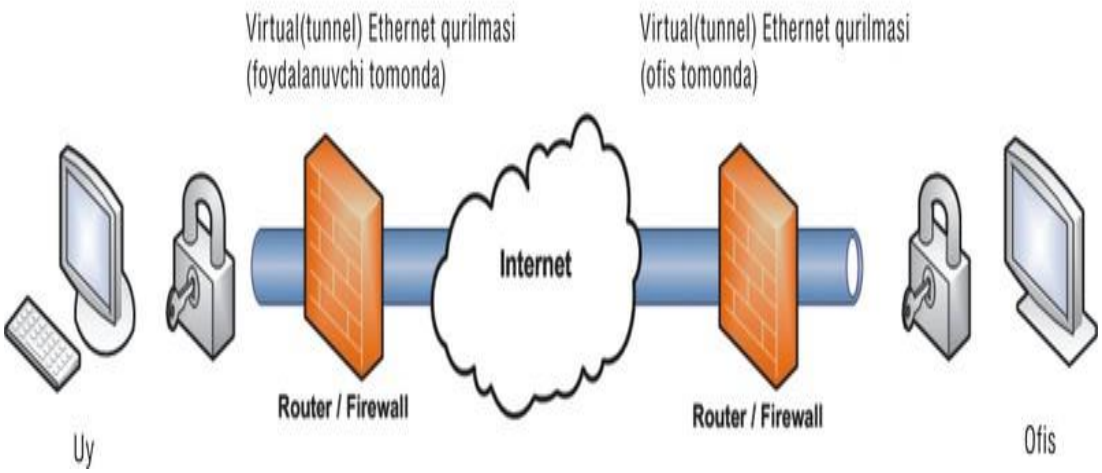
IPSec (Internet protocol security) bu xavfsizlik protokollari hamda shifrlash algoritmlaridan foydalangan holda tarmoq orqali xavfsiz ma’lumot almashish imkonini beradi. Bu maxsus standart orqali tarmoqdagi kompyuterlarning o‘zaro aloqasida dastur va ma’lumotlar hamda qurilmaviy vositalar bir-biriga mos kelishini ta’minlaydi. Ipsec protokoli tarmoq orqali uzatilayotgan axborotning sirliligini, ya’ni faqatgina yuboruvchi va qabul qiluvchiga tushunarli bo‘lishini, axborotning sofligini hamda paketlarni autentifikatsiyalashni amalga oshiradi. Zamonaviy axborot texnologiyalarni qo‘llash har bir tashkilotning rivojlanishi uchun zaruriy vosita bo‘lib qoldi, Ipsec protokoli esa aynan quyidagilar uchun samarali himoyani ta’minlaydi:

-bosh ofis va filiallarni global tarmoq bilan bog‘laganda;

-uzoq masofadan turib, korxonani internet orqali boshqarishda;

-homiylar bilan bog‘langan tarmoqni himoyalashda;

-elektron tijoratning xavfsizlik darajasini yuksaltirishda.



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 yerdan 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.

Ruxsatsiz kirishni aniqlash tizimi (IDS) yordamida tizim yoki tarmoq xavfsizlik siyosatini buzib kirishga harakat qilingan usul yoki vositalar aniqlanadi. Ruxsatsiz kirishlarni aniqlash tizimlari deyarli chorak asrlik tarixga ega. Ruxsatsiz kirishlarni aniqlash tizimlarining ilk modellari va prototiplari kompyuter tizimlarining audit

ma’lumotlarini tahlillashdan foydalangan. Bu tizim ikkita asosiy sinfga ajratiladi. Tarmoqqa ruxsatsiz kirishni aniqlash tizimi (Network Intrusion Detection System) va kompyuterga ruxsatsiz kirishni aniqlash tizimiga (Host Intrusion Detection System) bo‘linadi.

Xulosa

Xulosa qilib aytganda, yuqorida keltirib o`tilgan izlanishlar barchasi kompyuter tarmog`ining xavfsizligini ta`minlash uchun xizmat qiladi. 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 foydalanuvchilarga sezdirmagan holatda axborotlarni tinglash, o‘zgartirish hamda to‘sib qo‘yish mumkin. Bunda bir nechta tizim tarmog`i xavfsizligi xizmatlaridan foydalaniladi: Shifrlash, avtorizatsiya, audit va boshqalar

FOYDALANILGAN ADABIYOTLAR:

1.Olifer B., Computer Networking: Prinsiples, protocols and Practice. 2011.-282p

2.Qaxxarov A.A Tarmoqlarni rejalashtirish va qurish. O`quv qo`llanma-T..Noshir, 2012-224b

3.M.M.Musayev, A.A Qaxxarov, M.M.Karimov “ Kompyuter tarmoqlarini yig`ish”. “Ilm-ziyo” nashiryoti Toshkent-2011,176 b

4. Axborot xavfsizligini ta (tami.uz)

5. Axborot xavfsizligi - Vikipediya (wikipedia.org)