Emro Science and Education
Open-access scientific journal
Journal homepage: https://journal.emro.uz

OPEN ACCESS

CONFERENCE PAPER OPEN ACCESS

Vol. 1 No. 1 (2023) · “Axborot oqimlari va intellektual tizimlarning ijtimoiy, iqtisodiy va texnik-texnologik tarmoqlardagi o‘rni” mavzus...

materiallar to‘plami

KOMPYUTER TARMOG'I XAVFSIZLIGI MUAMMOLARI BO'YICHA TADQIQOTLAR VA QARSHI CHORALAR

Sh.B.Xamidova 1 bosqich magistranti. Andijon mashinasozlik instituti.

Kalit so'zlar: Tarmoq xavfsizligi, Internet, muammolar, viruslar xujumi, uskunalar, raqamli sertifikat, fayllar, maxfiy, shifrlash texnologiyasi.

Аннотация. Ushbu maqolada kompyuter tarmoq texnologiyasi xavfsizligining ahamiyati, tarmoq xavfsizligi muammolarining asosiy turlari bo`yicha hamda taxliliy natijalari , ularni amalda bajarish uchun qarshi choralar keltirilgan.

RESEARCH ON COMPUTER NETWORK SECURITY PROBLEMS AND COUNTERMEASURES

Sh.B. Shakirova is a 1st ear masters degree student. Andijan Institute of Mechanical Engineering

Keywords: Network security, Internet, problems and countermeasures Virus attack, equipment, Digital certificate, files, secret, encryption technology.

Abstract. This article presents the importance of computer network technology security, the main types of network security problems and analytical results, as well as countermeasures for their implementation.

ИССЛЕДОВАНИЕ И МЕРЫ ПРОБЛЕМЫ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ

Ш.Б.Шакирова – магистрантка 1 курса. Андижанский машиностроительный институт

Ключевые слова: Сетевая безопасность, интернет, проблемы, вирусная атака, оборудование, цифровой сертификат, файлы, секрет, технология шифрования.

Аннотацшя. В данной статье представлена важность обеспечения безопасности компьютерных сетевых технологий, основные виды проблем сетевой безопасности и аналитические результаты, а также меры противодействия их реализации.

Kirish. Internetning uzluksiz rivojlanishi natijasida, odamlar kompyuterlar va tarmoqlarsiz yashay olmaydi. Biroq, tarmoqdan foydalanish jarayonida, ko'pincha mavjud xavfsizlik muammolariga duch keladi. Bu foydalanuvchining tajriba hissini pasaytiradi va foydalanuvchilarning shaxsiy ma'lumotlarining xavfsizligiga tahdid soladi. Ushbu tadqiqot kompyuter tarmog'i xavfsizligi, xavfsizlik muammolarining o'ziga xos turlari va bir nechta samarali va qarshi choralar muhimligini muhokama qiladi. Bu esa kompyuter tarmoq xavfsizligi rivojlanishi uchun asos bo'lib xizmat qiladi.

1. Kompyuter tarmog'ining xavfsizligi

Xalqaro standartlashtirish tashkiloti kompyuter tarmog'i xavfsizligiga ta'rifni quydagicha beradi , bu o'rnatilgan texnologiya xavfsizligini ta`minlashning bir turi va apparat vositalarining kompyuter ma'lumotlarini yo'q qilish va oqib chiqishdan himoya qilish tizimlari , kutilmagan hamda yomon sabablarga ko'ra dasturiy ta`minotning

Published: 10.11.2023

Cite this article: Sh.B. Xamidova (2023). Kompyuter tarmog'i xavfsizligi muammolari bo'yicha tadqiqotlar va qarshi choralar. Emro Science and Education, 1(1). https://journal.emro.uz/public/maqola/595

© 2023 The Author(s). Published by Emro Science and Education. This is an open access article.

kompyuter ma`lumotlarini himoya qilish uchun bir qancha qayta ishlash tizimlaridan foydalaniladi . Kompyuter xavfsizligi ta'rifi jismoniy va mantiqiy xavfsizlikni o'z ichiga oladi [1].

Tarmoq xavfsizligi - bu Internetdagi ma'lumotlarning yaxlitligi va mavjudligini saqlash. Butunlik, ya'ni ruxsatsiz operatsiyalar ma'lumotlarni o'zgartira olmasligini ta'minlash. Samaradorlik, ya'ni ruxsatsiz operatsiyalar axborot yoki kompyuter resurslarini yo'q qila olmasligini ta'minlash. Sodda qilib aytganda, tarmoq tizimining xavfsizligi, tarmoq xavfsizligini hamda axborot xavfsizligini o'z ichiga oladi. Tarmoq xavfsizligi deganda tarmoqdan kelib chiqqan jismoniy liniyalar va ulanishlar xavfsizligi tushuniladi, tarmoqlar o'rtasida ishlash va o'zaro bog'lanish, operatsion tizim xavfsizligi, xodimlarni boshqarish xavfsizligi va boshqalar. Axborot xavfsizligi ma'lumotlarning xavfsizligini anglatadi, masalan, maxfiylik, haqiqiyligi, mavjudligi va boshqarilishi.



1Rasm. Xavfsizlik belgilari

Kompyuter tarmog'i xavfsizligining ahamiyati . Turli sohalarda kompyuter texnologiyalaridan keng foydalanish va avtomatlashtirishni rag'batlantirish bilan ish tizimi, an'anaviy ish rejimi tobora ko'proq e'tiroz bildirmoqda. Zamonaviy ofis ishi asta-sekin "qog'ozsiz" va "tarmoq" yo'nalishida rivojlanmoqda. Ayniqsa, Internet tijoratlashtirilgandan so`ng, Internet sanoati katta yutuqlarga erishdi [2].

Axborot tarmog'ining xalqarolashuvi, ochiqligi va shaxsiylashtirilishi nafaqatodamlarga "ma'lumot almashish" bilan ta'minlash, shuningdek, ishning yuqori samaradorligi va yuqori sifatini hayotimizga targ`ib etdi. Axborotni uzatish vaqt va makon bilan cheklanmaganligi sababli, tobora ko'proq kompyuterlar tarmoqqa ulanadi va hukumat va shaxslar asta-sekin tarmoqqa, tarmoq muhiti va tarmoq resurslariga tayanadi. Shu bilan birga, tarmoq tizimining xavfsizlik muammosi tobora ko'proq dolzarb bo'lib bormoqda tobora ko'proq e'tibor qaratmoqda. Onlayn ma'lumotlarning sizib chiqishi, o'zgartirilishi va qalbakilashtirilishi, viruslarning tarqalishi va yomon ma'lumotlarning tarqalishi, tarmoq uchun juda zararli xavf tug'diradi. Shundan kelib chiqadiki, kompyuter tarmog'ining xavfsizligi muammosini hal qilish o`ta muxim vazifalardan.

Kompyuter xavfsizligi muammolarining asosan ikki turi mavjud: 1) tizimdagi axborotga tahdidlar;

2) tizimdagi uskunalarga tahdidlar [3].

Kompyuter tizimiga ta'sir qiluvchi ko'plab omillar mavjud, ularning ba'zilari qasddan bo'lishi mumkin yoki tarmoqqa aloqador beixtiyor, texnogen, texnogen bo'lmagan yoki tabiiy sabablarga ko'ra sodir bo'lishi mumkin.

Kompyuter tizimlarining xavfsizligiga tahdidlar quyidagilar:

1. Ma'lumotlarni o'g'irlash. Xavfsizlik bo'shliqlari operatorlarning noto'g'ri xavfsizlik konfiguratsiyasi, past xavfsizlik xabardorligi tufayli yuzaga keladi foydalanuvchilar yoki foydalanuvchilarning o'z hisoblarini boshqalarga qarzga berishlari yoki baham ko'rishlari tarmoq uchun xavf tug'diradi. Bu juda ko'p ma'lumotlar yo'qotilishiga olib keladi. Ma'lumotlarning yo'qolishidan kelib chiqadigan yo'qotish behisob. Maxfiylik va mavjudlik tasodifiy xavf ostida qolishi mumkin [4].

2. Troyan oti virusi. Ko'pgina foydalanuvchilar tomonidan ishlatiladigan brauzerlar reklamalarni blokirovka qilish qobiliyatini sezilarli darajada yaxshilagan bo'lsa-da ba'zi antivirus dasturlari veb-saytlarining statistikasi brauzerlarning zaifligini yana bir bor aks ettiradi. Troyan oti - masofadan boshqarishga asoslangan xakerlik vositalarining bir turi bo'lib, uning xususiyatlariga ega yashirish va ruxsat bermaslik. Yashirish Troyan otining dizayneri bo'lishini anglatadi troyan otining bo'lishiga yo'l qo'ymaslik uchun, uni yashirish uchun turli xil choralarni ko'rish kashf etilgan. Agar foydalanuvchi troyan otini yuqtirganligini aniqlasa ham, uni muayyan joylashuvini aniqlash oson emas. Ruxsat bermaslik, boshqaruv tomoni server bilan bir marta ulanganligini bildiradi (hujum qilingan tomon) boshqaruv tomoni esa troyan dasturi orqali serverning ishlash huquqlarining katta qismini o'g'irlashi mumkin. Bunga fayllarni o'zgartirish, ro'yxatga olish kitobini o'zgartirish, dasturlarni ishga tushirish va boshqalar kiradi.

3. Zaifliklar. Ko'pgina tarmoq tizimlarida u yoki bu turdagi bo'shliqlar mavjud. Bu zaifliklar tizimga tegishli bo'lishi mumkin. Bundan tashqari, u rahbariyatning beparvoligi tufayli yuzaga kelishi ham mumkin. Bu zaifliklardan xakerlar turli hujumlar, jumladan, parolni aniqlash uchun foydalanishi mumkin.

Bundan tashqari, dasturiy ta'minot hujumi ular orasida keng tarqalgan usuldir. Xakerlar kompyuterning superfoydalanuvchi huquqlarini noqonuniy ravishda qo'lga kiritish va uni to'liq nazorat qilish imkoniyatiga ega. Fayllar bilan ishlashdan tashqari, u shuningdek, ish stolida tasvirlarni olishi, ko'plab ilovalarning parollarini va boshqa operatsiyalar ni olishi mumkin. Mijoz tomoni va server tomoni - bu dasturiy ta'minotning ikki xil turi. Xakerlar hujum qilganda, ular mijoz dasturlari yordamida tizimga kirishadi.

4. Mobil tahdid. Smartfon viruslari korporativ tarmoqlar va shaxsiy ma'lumotlarga tahdid soladi. Bugungi tarmoqni rivojlantirish tendentsiyasi nuqtai nazaridan tarmoq har qanday elektron mahsulotga ulanishi mumkin, va tarmoq hamma joyda ekanligi hujumlar ham hamma joyda ekanligini ko'rsatadi. Bundan tashqari, dastur tizimida apparat, operatsion tizim, tarmoqqa kirish uskunalari va bo'shliqlar bo'ladi. Mobil qurilmalarning saqlash joyidan foydalanish, yashash maydoni va inkubatsiya davri zararli kodni oldindan aytib bo'lmaydi.

5. Elektromagnit shovqin. Yuqori kuchlanishli simlar, radio to'lqin uzatuvchi antennalar, mikroto'lqinli yuqori chastotali elektron uskunalar va boshqalar elektromagnit shovqin signallarini ishlab chiqaradi. Bular elektromagnit shovqin

signallari kompyuter magnit muhitidagi ma'lumotni yo'q qiladi va shu bilan tarmoq xavfsizligiga ta'sir qiladi.

Har qanday tarmoq xizmati xavfsizlikka xavf tug'diradi, muammo xavfni qanday kamaytirishdir. Ayni paytda, tarmoq xavfsizligini himoya qilish choralari quyidagilardan iborat:

1. Tarmoqning xavfsiz muhitini yaratish. Xavfsiz tarmoq muhitini yaratish, jumladan, foydalanuvchilarni kuzatish, foydalanuvchini sozlash juda muhimdir ruxsatlar, kirishni boshqarish, identifikatsiya, monitoring routerlari va boshqalardan foydalanish.

2. Kompyuter viruslarini oldini olish. Kompyuter viruslari kompyuter dasturlaridagi bo'shliqlardan foydalanish orqali sun'iy ravishda yoziladi. Shuning uchun kompyuterning tez suratda rivojlanishi va yangi viruslarning paydo bo'lishi, uzatish tezligi kabilar borgan sari tezlashadi. Bundan tashqari, zarar ham tobora kuchayib boradi. Eng ko'p ishlatiladigan profilaktika kompyuter viruslariga qarshi chora - bu zararlangan fayllarni tekshirish va o'ldirish uchun antivirus dasturini o'rnatish.

Virusning oldini olish uchun quyidagi choralar ham mavjud:

1) Noma'lum dasturlar va ma'lumotlardan foydalanmaslik.
2) Noma'lum veb-saytlardan fayllarni xohlagancha yuklab olmaslik.
3) Faylni yuklab olgandan so'ng, uni ishlatishdan oldin virusni dezinfeksiya qilish.
4) Noma'lum kelib chiqishi (ilova) do'kon manzilining elektron pochtasini osongina ochmaslik.
5) Ko'pincha muhim ma'lumotlarning zaxira nusxasini yaratish va hokazo.
6) Viruslar sonini kamaytirish uchun tizimni yangilash yamoqlarini tez-tez o'rnatish.

3. Firewall texnologiyasi. Xavfsizlik devori - bu turli xostlar, foydalanuvchilar yoki pastki tarmoqlarning tarmoq xavfsizligini himoya qilish uchun ishlatiladigan tizim. Xavfsizlik devorining asosiy vazifasi turli pastki tarmoqlar o'rtasida xavfsiz kirish siyosatini amalga oshirish va qo'llashdir [5]. Xavfsizlik devori foydalanuvchi tarmog'ini funksiya va xavfsizlik darajasiga ko'ra turli pastki tarmoqlarga ajratadi va xavfsizlik devori orqali kirishni boshqarishni amalga oshiradi.

Intranet - bu ishonchli tarmoq. U Internet kabi tashqi tarmoqlarga xavfsizlik devorlari orqali kirishi mumkin. Shuningdek, u xavfsizlik devori, ya'ni umumiy tarmoq orqali xizmatlar ko'rsatadigan tarmoqqa , xavfsizlik pastki tarmog'i orqali kirishi mumkin. Xavfsizlik devori orqali pastki tarmoqlar orasidagi kirishni boshqarish, turli xil xavfsizlik darajalari va zararli yoki ruxsatsiz kirishning oldini olish uchun mumkin [6].

4. Ma'lumotlarni shifrlash. Tarmoq xakerlari tizimga bostirib kirishi sababli, ma'lumotlarni o'g'irlashi yoki tarmoqdagi ma'lumotlarni tinglashi mumkin.
Ma'lumotlar shifrlash orqali o'g'irlangan ma'lumotlar shunchaki ochilmaydi, bu esa yo'qotishni biroz kamaytiradi. Hozirgi vaqtda shifrlash texnologiyasi nisbatan etuk bo'lib, shifrlashning ikki turi mavjud tez-tez ishlatiladigan texnologiyalar: 1) Simmetrik kalitlarni shifrlash texnologiyasi.
2) Ochiq kalitlarni shifrlash texnologiya.

5. Raqamli imzo. Raqamli imzodan xabar jo'natuvchi tomonidan berilganligini tekshirish uchun foydalanish mumkin. Bundan tashqari, raqamli imzo ma'lumotlarni yoki dasturni saqlash uchun ishlatilsa, uni isbotlash uchun ma'lumotlar yoki dasturning yaxlitligidan ham foydalanish qo`l keladi. Oddiy qo'lda yozilgan imzolar singari, undan foydalanish ma'lumotlarning haqiqiyligini tekshirish imkoniyati mavjud.

6. Ma'lumotlarning haqiqiyligini. Onlayn ID karta bilan taqqoslaganda, raqamli sertifikat haqiqiylik funktsiyasiga ega bo'lgan uchinchi tomon vakolatli autentifikatsiyasi orqali Internetda shaxsni tasdiqlash uchun raqamli imzodan foydalanadi. Raqamli sertifikatlar xavfsiz, maxfiy, o'zgartirishdan himoyalangan va korxona ma'lumotlarini samarali himoya qiladi [7].

Xulosa. Insoniyat kompyuter tarmog'ining xavfsizligiga tobora ko'proq e'tibor berishmoqda. Vaziyatga ko'ra tarmoq xavfsizligi sanoatining jadal rivojlanishi va axborot jarayonining tezlashishi, turli xil yangi texnologiyalarni qo'llashda davom etadi. Tarmoq xavfsizligi cheksiz imkoniyatlarga boy, tadqiqotchilar uchun issiq hududga aylanganligi sababli, uning rivojlanishi katta strategik ahamiyatga ega va kelajakda tarmoq xavfsizligi texnologiyasi yanada sezilarli yutuqlarga erishadi. Tadqiqotchilar kerak oqilona maqsadlar va tegishli qonunlarni belgilash uchun, xavfsizlik omillarini to'liq amalga oshirish maqsadida kerak.

Foydalanilgan adabiyotlar

[1]. Yang Guang, Li Feifei, Yang Yang; Analysis of computer network security measures [J]; Science & Technology Information; 2011.

[2]. Yang Shuxin; Research on Computer Network Safety Technology [J]; Journal of Hebei Energy Institute of Vocation and Technology; 2008.

[3]. Ren Xingzhou; The Analysis and Solutions to Computer Net Security [J]; Computer Knowledge and Technology; 2005.

[4]. U Zhang Suying; An Inquiry into Hidden Danger in Network Safety and the Safety Precautions [J]; The Science Education Article Collects; 2012.

[5]. Xiong Fangfang; A brief discussion on the problems of computer Network Security and its Countermeasures [J]; Electronics World; 2012.

[6]. Wang Tian, Xiao Hui; Defense Technology of Network Safety and It’s Development [J]; Journal of Anhui Vocational College of Metallurgy and Technology; 2007.

[7]. Changjiang. Research on Computer Network Security Problems and Countermeasures. Politexnika, Wuhan, Hubei, China. 2021.