TARMOQ XAVFSIZLIGI

Ismatova Shohsanam Xamzayevna
Samarqand viloyati Pastdarg'om tumani
12-maktab informatika fani o'qituvchisi.

Annotatsiya : *Usbu maqolada tarmoq xavfsizligi tarmog'ingiz va ma'lumotlaringizni buzilishlar, bosqinlar va boshqa tahdidlardan himoya qiladi. Bu apparat va dasturiy echimlarni, shuningdek, tarmoqdan foydalanish, foydalanish imkoniyati va tahdidlardan umumiy himoya bilan bog'liq jarayonlar yoki qoidalar va konfiguratsiyalarni tavsiflovchi keng va keng qamrovli atama.*

Kalit so'zlar: *axborot xavfsizligi, kiber ataka, tarmoq skanerlari, tarmoq shifferlari, autentifikatsiy, access control, kriptotizim.*

KIRISH

Tarmoq xavfsizligi doirasida har qanday tarmoq xavfsizligi strategiyasining asosi bo'lishi kerak bo'lgan uchta asosiy yo'nalish mavjud: himoya qilish, aniqlash va javob berish. Himoyatarmoq xavfsizligiga tajovuzni oldini olish uchun mo'ljallangan har qanday xavfsizlik vositalari yoki siyosatlarini o'z ichiga oladi. Aniqlashtarmoq trafigini tahlil qilish va muammolarni zarar yetkazishidan oldin tezda aniqlash imkonini beruvchi resurslarni nazarda tutadi. Javobberish- aniqlangan tarmoq xavfsizligi tahdidlariga javob berish va ularni imkon qadar tezroq hal qilish qobiliyati. Afsuski, aksariyat korxonalar siyosatga qanday amal qilishni va buni to'g'ri bajarishni bilishmaydi. AQSH va Yevropa bo ylab 4100 nafar rahbar, bo lim‘‘ boshliqlari, IT-menejerlari va boshqa muhim mutaxassislar ishtirokida o tkazilgan‘ so rovda ma lum bo ldiki, har to rt tashkilotdan deyarli uch nafari (73 foiz) 3 nafari‘’‘‘ yangi darajadagi kiberxavfsizlik strategiyasini ishlab chiqmoqda. Bu tobora kuchayib borayotgan tahdiddir, chunki tarmoq buzilishi sodir bo'lganda va zararli tahdidlar paydo bo'lganda, faqat ma'lumotlarning o'zi emas, balki ko'proq xavf tug'diradi.

Internet texnologiyalarining yaratilishi turli manbalardan tez va oson yo'l bilan axborot olish imkoniyatlarini hamma uchun-oddiy fuqarodan tortib yirik tashkilotlargacha misli ko'rilmagan darajada oshirib yubordi. Davlat muassasalari, fan-ta'lim muassasalari, tijorat korxonalari va alohida shaxslar axborotni elektron shaklda yaratib-saqlay boshladilar. Axborotdan samarali foydalanish imkoniyatlari axborot miqdorining tez ko'payishiga olib keldi. Biznes qator tijorat sohalarida bugun axborotni o'zining eng qimmatli mulki deb biladi. Bu albatta ommaviy axborot va hamma bilishi mumkin bo'lgan axborot haqida gap borganda o'ta ijobiy hodisa. Lekin maxfiy axborot oqimlari uchun Internet texnologiyalari qulayliklar bilan bir qatorda yangi muammolar keltirib chiqardi. Internet muhitida axborot xavfsizligiga tahdid keskin oshdi. Tajovuzlarni tashkil etish shakllari har xil bo'lib ular quyidagi turlarga bo'linadi:

- Kompyuterga olisdan kirish - Internet yoki intranetga kimligini bildirmay kirishga imkon beruvchi dasturlar. O'zi ishlab turgan kompyuterga kirish: kompyuterga kimligini bildirmay kirish dasturlari asosida.

● Kompyuterni olisdan turib ishlatmay qo'yish - Internet tarmog'i orqali olisdan kompyuterga ulanib, uning yoki uni ayrim dasturlarining ishlashini to'xtatib qo'yuvchi dasturlar asosida(ishlatib yuborish uchun kompyuterni qayta ishga solish yetarli).

● O'zi ishlab turgan kompyuterni ishlatmay qo'yish - ishlatmay qo'yuvchi dasturlar vositasida.

●Tarmoq skanerlari - tarmoqda ishlayotgan kompyuter va dasturlardan qay biri tajovuzga chidamsizligini aniqlash maqsadida tarmoq haqiqatda axborot yig'uvchi dasturlar vositasida.

● Dasturlarning tajovuzga bo'sh joylarini topish - Internetdagi kompyuterlarning katta guruhlari orasidan tajovuzga bardoshsizlarini izlab qarab chiquvchi dasturlar vositasida.

● Parol ochish - parollar fayllaridan oson topiladigan parollarni izlovchi dasturlar vositasida.

●Tarmoq tahlilchilari (snifferlar) - tarmoq trafikini tinglovchi dasturlar vositasida. Ularda foydalanuvchilarning nomlarini, parollarini, kredit kartalari nomerlarini trafikdan avtomatik tarzda ajratib olish imkoniyati mavjud.

Inkor eta olinmaslik(Neoproverjimost) - Ma'lumotlar massivini jo‘natuvchi tomonidan uni jo‘natganligini yoki oluvchi tomonidan uni olganligini tan olishdan bo‘yin tovlashining oldini olish. Ko‘plab qo‘shimcha xizmatlar (audit, kirishni ta'minlash) va qo‘llab-quvvatlash xizmatlari (kalitlarni boshqarish, xavfsizlikni ta'minlash, tarmoqni boshqarish) mazkur asosiy xavfsizlik tizimini to‘ldirishga xizmat qiladi. Web tugunining to‘la xavfsizlik tizimi barcha yuqorida keltirilgan xavfsizlik yo'nalishlarini qamrab olgan bo'lishi shart. Bunda tegishli xavfsizlik vositalari (mexanizmlari) dasturiy mahsulotlar tarkibiga kiritilgan bo‘lishi lozim.

Autentifikatsiyalashni takomillashtirish qayta ishlatiladigan parollarga xos kamchiliklarni bartaraf etishni, shu maqsadda bir martagina ishlatiladigan parol tizimidan tortib identifikatsiyalashning yuqori texnologik biometrik tizimlarigacha qo‘llashni nazarda tutadi. Foydalanuvchilar o‘zlari bilan olib yuradigan predmetlar, masalan, maxsus kartochkalar, maxsus jeton yoki disketa ancha arzon ham xavfsiz. Noyob, modul kodi himoyalangan dastur moduli ham bu maqsadlarda qulay. Oshkor kalitlar infratuzilmasi ham Web – tugun xavfsizligining ajralmas qismi. Autentifikatsiya, ma'lumot butunligi va axborotpinhonaligi(konfidentsialligi)ni ta'minlash uchun ishlatiladigan taqsimlashga tizim(odamlar, kompyuterlar), Ochiq kalit infrastrukturali (sertifikat nashrchisi) elektron sertifikatni e'lon qiladi. Unda foydalanuvchi identifikatori, uning ochiq kaliti, xavfsizlik tizimi uchun qandaydir qo‘shimcha axborot va sertifikat nashr etuvchisining raqamli imzosi bor. Ideal variantda bu tizim Yer yuzining har qanday ikki nuqtasidagi foydalanuvchi uchun sertifikatlar zanjirini tuzib beradi. Bu zanjircha kimgadir maxfiy xatni imzolash, hisob bo‘yicha pul o‘tkazish yoki elektron kontrakt tuzish uchun, boshqa kishi uchun–hujjat manbaini va imzolovchi shaxsning aslini tekshirib bilish imkonini beradi. NIST bir necha boshqa tashkilotlar bilan bu yo‘nalishda ish olib bormoqda. Internetga ulangan tarmoqlar xakerlarning tajovuzi tufayli ochiq muloqotga xalal bersa xam brandmauerlar o‘rnatib oldilar.

PGP ga o‘xshash mukammal dasturlar bo‘lmaganda ochiq tarmoq bo‘lishi ham mumkin bo‘lmas edi.

Tarmoqni kompyuter tajovuzlaridan himoyalash doimiy va o'z-o'zidan yechilmaydigan masaladir. Lekin qator oddiy himoya vositalari yordamida tarmoqqa suqulib kirishlarning ko'pchiligini oldini olish mumkin. Masalan yaxshi konfiguratsiyalangan tarmoqlararo ekran va harbir ish stantsiyalari(kompyuterlar)da o'rnatilgan virusga qarshi dasturlar ko'pchilik kompyuter tajovuzlarini barbod etadi. Quyida Intranetni himoyalash bo'yicha 14 amaliy tavsiya bayon etilgan. Xavfsizlik siyosati lo'nda va aniq qo'yilishi lozim. Intranet tarmog‘i xavfsizligi bo‘yicha yorqin va sobit qadamlik bilan qo‘yilisini ta'minlaydigan qoidalar va amallar bo’lishi lozim. Tarmoq xavfsizligi tizimi uning eng bo'sh joyi qanchalik kuchli himoyalangan bo'lsa shu qadar kuchlidir. Agar bir tashkilot doirasida turli xavfsizlik siyosatlariga ega bo'lgan bir necha tarmoq mavjud bo'lsa bir tarmoq boshqa tarmoqning yomon xavfsizligi tufayli obro'sini yo'qotishi mumkin. Tashkilotlar shunday xavfsizlik siyosatini qabul qilishlari lozimki, kutilgan himoya darajasi hamma yerda bir xil amalga oshsin. Siyosatning eng ahamiyatli tomoni brandmauerlar orqali o'tkaziladigan trafiklarga yagona talab ishlab chiqilishidir. Shuningdek siyosat tarmoqda qaysi himoya vositalari (masalan, tajovuzlarni payqash vositalarimi yoki qaltis joylar skanerlarimi)va ular qanaqa ishlatilishi lozimligini belgilashi, yagona xavfsizlik darajasiga erishish uchun kompyuterlarning har xil turlari uchun standart xavfsiz konfiguratsiyalar belgilanishi shart. Brandmauer (Tarmoqlararo ekran, inglizcha-firewalls,) qo'llash lozim. Bu tashkilotning eng asosiy himoya vositasidir. Tarmoqqa kiruvchi, undan chiquvchi trafik(axborot oqimi)ni nazorat qiladi. U trafikning biror turini to'sib qo'yishi yo tekshirib turishi mumkin. Yaxshi konfiguratsiyalangan bradmauer kompyuter tajovuzlarining ko'pchiligini qaytarishi mumkin. brandmauerlar, intellektual kartalar va boshqa texnikaviydasturiy himoya vositalaridan oqilona foydalanish lozim.

FOYDALANILGAN ADABIYOTLAR:

1. Маллабоев Н., Шокиров Д. СПОСОБЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ //Теория и практика современной науки. – 2016. – №. 6-1. – С. 826-830.

2. Маллабоев Н., Шокиров Д. СИСТЕМЫ ЭЛЕКТРОННОГО ПЛАТЕЖА //Теория и практика современной науки. – 2016. – №. 6-1. – С. 830-834.

3. Abdullaeva N., Mamurova F., Mallaboev N. EFFICIENCY OF EXPERIMENTAL PREPARATION USE MULTIMEDIA TO ENLARGE SOME QUESTIONS //Экономика и социум. – 2020. – №. 6. – С. 11-13.