UDK 004

Mallaboyev N.
katta o'qituvchi
Umarova G.
katta o'qituvchi
Namangan muhandislik-qurilish instituti

AXBOROT XAVFSIZLIGI MUAMMOLARI

Annotatsiya: usbu maqolada mualliflar axborot xavfsizligi, uning turlari vazarazkash darajasi xaqida tahlil olib borishgan.

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

Mallaboyev N.
senior lecturer
Umarova G.
senior lecturer
Namangan Institute of Engineering and Construction

INFORMATION SECURITY ISSUES

Abstract: in this article, the authors conducted an analysis of information security, its types and level of security.

Keywords: information security, cyber attack, network scanners, network ciphers, authentication, access control, cryptosystem.

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.

Eng ko'p yuz beradigan tajovuzlar quyidagi statistikaga ega:

1998 yili NIST tomonidan o'tkazilgan 237 kompyuter tajovuzining tahlili Internetda e'lon qilingan:

29% tajovuzlar Windows muhitida yuz bergan.

Saboq: Faqat Unixgina xatarli emas ekan.

20% tajovuzlarda tajovuz qilganlar olisdan turib tarmoq elementlari(marshrutlovchilar, kommutatorlar, xostlar, printerlari brandmauer) gacha yetib borganlar.

Saboq: xostlarga olisdan turib bildirmay kirish bot-bot yuz beradi.

5% tajovuzlar marshrutlovchilarga va brandmauerlarga qarshi muvaffaqiyatli bo'lgan.

Saboq: Internet tarmoq infrastrukturasi tashkil etuvchilarining kompyuter tajovuzlariga bardoshi yetarli emas.

4% tajovuzlarda Internetda tajovuzga bardoshi bo'sh xostlarni topish uchun uyushtirilgan.

Saboq: Tizim administratorlarining o'zlari o'z xostlarini muntazam skanerlab turganlari ma'qul. 3% tajovuzlar web-saytlar tomonidan o'z foydalanuvchilariga qarshi uyushtirilgan.

Saboq WWWda axborot izlash xavfsiz emas.

2021 yilda:

- Norvegiyaning eng yirik gazetalari xakerlik hujumlari tufayli yopildi
- Hackerlar Dnevnik.ru saytini buzib, maktab o'quvchilarining baholarini o'zgartirdilar
- 1,6 million WordPress veb-saytlari hujumga uchradi
- Volvo avtomobillarini sindirish

- Braziliyalik avtosug'urta kompaniyasi Porto Seguro xakerlik hujumiga uchradi
- 5 kiberfiribgarlik hujumlaridan 1 tasi davlat idoralariga qaratilgan
- Katta kiberhujumdan so'ng Olympus o'zining IT tizimlarini yopib qo'ydi
- T&L sohasidagi kiberhujumdan ko'rilgan zarar 50 million dollar yoki undan ko'proqqa yetishi mumkin
- yil davomida butun dunyo bo'ylab korxonalarga kiberhujumlar xavfi 24% ga oshdi
- Xakerlar Qozog‘iston elektron hukumati saytiga virus dasturini yuklagan, uni foydalanuvchilar yuklab olgan
- Xakerlar Belarus pasportining IT tizimini buzishdi
- Luma Energy yirik energetika kompaniyasi kiberhujumlarga uchradi
- Dunyodagi eng yirik go'sht ishlab chiqaruvchi JBS kompaniyasiga xaker hujumi
- Xakerlar 2 yil davomida Belgiya Ichki ishlar vazirligi tarmog‘ida jimgina “o‘tirishdi” va xodimlarning xatlarini o‘qishdi.
- Avtomobil ehtiyot qismlari ishlab chiqaruvchi Toyota Auto Body kompaniyasiga kiberhujum
- Hackerlar Vashington politsiyasining IT tizimlariga buzib kirishdi va hujjatlarni o'g'irlashdi
- Belarus AES veb-sayti buzilgan
- SolarWinds serverlaridan biri oddiy parol bilan himoyalangan
- SolarWinds kiberhujumlari tarixdagi eng yirik - Microsoft

2022 yilda:

- Firibgar Verizon’ning yuzlab xodimlarining ma’lumotlarini o‘g‘irlaydi
- "Kosmik qaroqchilar" Rossiya aerokosmik sanoatiga hujum qilmoqda
- Estoniya hukumati veb-saytlari hujum ostida
- Bolgaria Post kiberhujumga uchradi
- Ukrtelecom keng ko'lamli kiberhujumga uchradi
- Xakerlar “Miratorg” go‘sht xoldingining axborot resurslariga hujum qilishdi
- Braziliyalik xakerlar Ubisoft-ni buzishdi
- Kuzatuv tizimini ishlab chiqaruvchi Axis kiberhujumga uchradi
- Nvidia xakerlar tomonidan hujumga uchradi
- Kiberhujum tufayli Yaponiyaning barcha Toyota Motor zavodlarida ishlab chiqarish to'xtatildi

NIST 7498-2 xalqaro standarti asosiy xavfsizlik xizmatlarini belgilaydi. Uning vazifasiga ochiq tizimlar aloqasi modelining xavfsizlik yo’nalishlarini aniqlash kiradi. Bular:

Autentifikatsiya - Kompyuter yo tarmoq foydalanuvchisining shaxsini tekshirish;

Kirishni boshqarish(Access control) - Kompyuter tarmog‘idan foydalanuvchining ruxsat etilgan kirishini tekshirish va ta’minlash;

Ma’lumotlar butunligi - Ma’lumotlar massivi mazmunini tasodifiy yo qasddan beruxsat usullar bilan o‘zgartirishlarga nisbatan tekshirish;

Axborot pinhonaligi - Axborot mazmunini iznsiz oshkor bo‘lishdan himoyalash

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 axborot pinhonaligi(konfidentsialligi)ni ta’minlash uchun ishlatiladigan taqsimlashga n 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 texnikaviy-dasturiy himoya vositalaridan oqilona foydalanish lozim.

Brandmauer va WWW-serverlarni ularning ishini to'xtatib qo'yish tahdidlariga qarshi bardoshliligini testdan o'tkazib turish lozim. Internetda kompyuterning ishini to'xtatib qo'yishga yo'naltirilgan tajovuzlar tarqalgan. Tajovuzkorlar doimo WWW-saytlarni ishdan chiqaradilar, kompyuterlarni ortiq vazifalar bilan yuklab qo'yadilar yoki tarmoqlarni ma'nosiz paketlar bilan to'ldirib tashlaydilar. Bu turdagi tajovuzlar juda jiddiy bo'lishi mumkin, ayniqsa tajovuzkor davomli tajovuzlarni uyushtirish darajasida aqlli bo'lsa. Chunki buning manbaini topib bo'lmaydi. Xavfsizligi haqida qayg'iruvchi tarmoqlar bunday tajovuzlardan ko'riladigan zararni chamalab ko'rish uchun o'zlariga o'zlari tajovuzlarni uyushtirishlari mumkin. Bunday tahlillarni faqat katta tajribaga ega tizim administratorlari yoki maxsus maslahatchilar o'tkazishi maqsadga muvofiq. Kriptotizimlardan keng foydalanish lozim. Tajovuzkorlar ko'pincha tarmoqqa uning ahamiyatga molik joylaridan o'tuvchi trafigini tinglash orqali trafikdan foydalanuvchilarni va ularning parollarini ajratib olish yordamida suqulib kiradilar. Shuning uchun olisdagi mashinalar bilan bog'lanishlar parol bilan himoyalanganda shifrlanishi shart. Bu ayniqsa, bog'lanish Internet kanallari orqali amalga oshirilganda yoki ahamiyatli server bilan bog'lanilganda zarur. TCP/IP (eng mashhuri SSH) trafigini shifrlash uchun tijoratli va bepul dasturlar mavjud. Bulardan foydalanish tajovuzlarning oldini oladi. Internet muhit bilan birlashgan Intranetda axborot oqimini va resurslarni eng ishonchli himoyalash vositasi–nosimmetrik va simmetrik kriptotizimlardan birgalikda foydalanishdir. Kompyuterlarni xavfsizlik nuqtai-nazaridan savodxonlarcha konfiguratsiyalash kerak. Kompyuterda amal tizimlari yangitdan o'rnatilganda ko'pincha tajovuzlarga qaltis bo'ladilar.Buning sababi amal tizimi dastlab o'rnatilganda barcha tarmoq vositalaridan foydalanishga

ruhsat beriladi va ulardan to'g'ri foydalaniladi deb bo'lmaydi. Bu tajovuzkor uchun mashinaga tajovuz uyushtirishda ko'p usullardan foydalanishga yo'l ochadi. Shuning uchun barcha zarur bo'lmagan tarmoq vositalari kompyuterdan uzib qo'yilishi lozim. Dasturiy ta'minotga tuzatishlarni operativ kiritishni tartibga solish(Patching). Kompaniyalar bot-bot o'z dasturlarida topilgan xatolarni yo'qotish uchun tuzatishlar kiritib boradilar. Agar bu xatolar tuzatilmasa tajovuzkor undan foydalanib dasturingizga va u orqali kompyuteringizga tajovuz uyushtirishi mumkin. Tizim administratorlari avvalo o'zlarining eng zarur tizimlaridagi dasturlarga tuzatishlarni o'rnatib zarur xostlarni himoyalashlari zarur. Chunki tuzatishlar tez-tez yuzaga kelib turadi va ularni barcha kompyuterlarda o'rnatib chiqishga ulgurmay qolish mumkin. Odatda tuzatishlar faqat dastur ishlab chiqargan korxonadangina olinishi shart. Intranet-tarmoq xavfsizligida uchratilgan defektlarni albatta tuzatish. Shuning bilan birga quyida keltirilgan boshqa himoya vositalaridan ham foydalanishlari zarur. Tajovuzni payqash vositalari (Intrusion Detection)dan foydalanish lozim. Tajovuzni payqash tizimlari tajovuzlarni operativ payqab aniqlaydilar. Tarmoq ichkarisidan bo'ladigan tajovuzlarni payqash uchun ular brandmauer orqasiga qo'yiladi, branmauerga bo'ladigan tajovuzlarni aniqlash uchun esa-uning oldiga o'rnatiladi. Xavfsizlikka oid tavsiyalar–kompyuter jinoyatlariga qarshi kurash guruhlari va dastur ishlab chiqaruvchilar tomonidan yaqin orada payqalgan dasturning qaltis joylari haqida e'lon qilinadigan ogohlantirishlar. Tavsiyalar juda foydali bo'lib, o'qish uchun juda kam vaqt oladi va payqab qolingan qaltis joylar tufayli yuzaga kelishi mumkin bo'lgan eng jiddiy xavf-xatarlardan ogoh etadi. Ular xavf-xatarni ifodalab uning oldini olish uchun maslahatlar beradi. Ularni qator joylardan olish mumkin. Ikkita eng foydali bo'lgan tavsiyalar kompyuter jinoyatlariga qarshi kurash guruhi e'lon qilib turadigan tavsiyalar bo'lib CIAC va CERT saytlaridan olish mumkin. Xavfsizlik bilan bog'liq hodisalarni tekshirish guruhi muntazam faoliyat olib borishi lozim. Har qanday tarmoqda ham xavfsizlik billan bog'liq hodisalar sodir bo'lib turadi(yolg'on trevoga bo'lsa ham). Tashkilot xizmatchilari avvaldan u yo bu holda nima qilishni bilishlari shart. Qaysi hollarda huquqiy-himoya organlariga murojaat qilish kerak, qaysi hollarda kompyuter jinoyatlariga qarshi kurash guruhini chaqirish va qaysi hollarda tarmoqni Internetdan uzib qo'yish kerak va ahamiyatli serverning qulfi buzilganda nima qilish kerak. CERT AQSH doirasida bu borada maslahatlar beradi. FedCIRC AQSH jamoat va davlat tashkilotlariga maslahatlar berish uchun mas'uldir. Harbir davlatda bunday maslahat olish joylari bo'lishi maqsadga muvofiqdir.

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.