SOTISH-PLATFORMALARNING KIBERXAVSIZLIKKA TA’SIRI VA XAVFSIZLIKNING MUTAHKAMLANISHI

Quldoshev Otabek Zarif o’g’li

Muhammad al-Xorazmiy nomidagi

Toshkent axborot texnologiyalari universiteti

Nurafshon filiali 2-kurs talabasi

Tel: +998908777399

kuldoshevotabek87@gmail.com

Annotatsiya: Sotish-platformalarning kiberxavfsizlikka ta'siri va xavfsizlikning mustahkamlanishi mavzulari tahlil qilinadi. Sotish-platformalar, ma'lumotlarni almashish va shaxsiy ma'lumotlarni saqlash uchun yuqori darajada xavfsizlik ta'minlash zarurati bilan bog'liqdir.

Kalit so’zlar: Elektron do’konlar, sotish platformalari, zararli viruslar, axborot vositalar.

Sotish-platformalar va Kiberxavfsizlik: Sotish-platformalar, onlayn savdo platformalari, elektron do'konlar va boshqa internet orqali sotish tizimlari uchun xavfsizlik o'rnini ta'minlashda muhim rol o'ynaydi. Ularning xavfsizlikni ta'minlashi va ma'lumotlarni himoya qilishlari sotish qiluvchilarning ishonchini oshiradi va ularni kiber xavf va hamjihatdan himoya qiladi. Kiberxavfsizlikga Ta'sir: Kiberxavfsizlik masalalari sotish-platformalar uchun katta muammo bo'lib, ma'lumotlar to'plash, saqlash va uni tahlil qilish, to'lov jarayonlarini himoya qilish kabi jarayonlarda xavfsizlikni ta'minlash zarurati bor. Kiberatakalar, identifikatsiya va to'lov ma'lumotlariga hujumlar kiritish, shaxsiy

ma'lumotlarni olish va boshqa xavfli faoliyatlar yuzaga kelishi mumkin. Xavfsizlikning Mustahkamlanishi: Sotish-platformalarning kiberxavfsizlikni ta'minlash uchun turli usullarni qo'llab-quvvatlashi zarur. Bu usullar o'z ichiga xavfsizlik so'rovnomalarini mustahkamlash, ma'lumotlar almashish va saqlash protokollarini shifrlash, identifikatsiya jarayonlarini ta'sir ostida qilish, yagona kirish nuqtalarini himoya qilish kabi tashqi xavfsizlik ta'minoti bo'lishi mumkin. Sotish-platformalar va Xalqaro Xavfsizlik Standartlari: Sotish-platformalar kiberxavfsizlik sohasidagi xalqaro standartlarni amalga oshirishadi. Misol uchun, PCI DSS (To'lov Karta Sifatli To'lovlarni Himoya Qilish So'rovnomasi), GDPR (Maxfiylik Kuzatuv Vaqti, Hisobingizni boshqarish so'rovnomasi), va boshqa standartlar ma'lumotlarni himoya qilish uchun yordam beradi va foydalanuvchilar uchun ishonch yaratadi. Sotish-platformalarning Kiberxavfsizlik Strategiyalari: Sotish-platformalar kiberxavfsizlikni o'zlarining strategiyalari bilan qo'llab-quvvatlashlari zarur. Bu strategiyalar ma'lumotlarni himoya qilish, ma'lumotlar to'plash protsesslarini kuzatish, xavfsizlik ta'sirini aniqlash va ta'sir ostida qilishni ta'minlashni o'z ichiga oladi.

Ma'lumotni qanday himoya qilish kerak? Turli xil axborot bilan tahdidlarning doimiy o'sishi va jadal rivojlanayotganiga qaramay, hanuzgacha himoya usullari mavjud. Jismoniy himoya -bu axborot xavfsizligining birinchi bosqichi. Bunga kirish cheklovini o'z ichiga oladi xorijiy foydalanuvchilar va o'qitish, ayniqsa, server blokiga kirish uchun. Axborot xavfsizligining asosiy darajasi -bu kompyuter viruslarini to'sib qo'yadigan dasturlar va antivirus dasturlari, Shubhali yozishni filtrlash tizimi. Dasturiy ta'minotni ishlab chiquvchilar taklif qiladigan DDOS hujumlaridan himoya qilish. Jonzot zaxira nusxalariboshqa tashqi muhitda yoki "bulut" da saqlanadi. Favqulodda vaziyatlar rejasi va ma'lumotlarni tiklash. Ushbu usul o'zlarini himoya qilishni va muvaffaqiyatsiz bo'lsa, bo'sh vaqtni kamaytiradigan yirik kompaniyalar uchun muhimdir. Elektron ommaviy axborot vositalaridan foydalanayotganda ma'lumotlarni shifrlash Axborotni himoya qilish integratsiyalashgan yondashuvni talab qiladi. Va nima katta miqdor Usullar qo'llaniladi, ma'lumotlarga yoki ma'lumotlarga zarar etkazish yoki ularga zarar etkazish uchun ruxsatsiz kirish huquqidan samaraliroq samarali bo'lgan. O'ylashga majbur bo'lgan bir

nechta faktlar 2016 yilda DDOS hujumlari banklarning 26 foizida qayd etildi. Shaxsiy ma'lumotlarni eng katta etishmovchiligidan biri 2017 yil iyul oyida Kredit tarixi byurosi (AQSh) da sodir bo'ldi. 143 million kishi va 209 mingta kredit karta raqamlari tajovuzkorlarning qo'liga tushdi. Ushbu bayonot, ayniqsa qachon o'z dolzarbligini yo'qotmadi biz gaplashyapmiz raqobat haqida. Shunday qilib, 2010 yilda iPhone 4-ning taqdimoti, ishchilar barda smartfonning prototipini unutib, talabalarga jurnalistlarga prototipni sotdi. Natijada, rasmiy taqdimotidan bir necha oy oldin ommaviy axborot vositalarida smartfonning eksklyuziv sharhi chiqdi. Yangi axborot texnologiyalariva universal kompyuterlashtirishning rivojlanishi Axborot xavfsizligi nafaqat majburiy bo'lmasligiga olib keldi, bu ham IP ning xususiyatlaridan biridir. Xavfsizlik omili asosiy rolni (masalan, bank axborot tizimlari) o'tkazadigan juda keng keng qamrovli ma'lumotlar to'plami mavjud.

Xavfsizlik ostida. Tizimning xavfsizligi yoki qasddan aralashuvdan, uning tarkibiy qismlarini o'g'irlash, o'zgartirishlar yoki uning tarkibiy qismlarini ruxsatsiz qabul qilishdan iborat bo'lganligi), uning ishlashi yoki qasddanfoydalanishning normal holatida tushuniladi. Boshqacha aytganda, IP-ga turli xil bezovta qiluvchi ta'sirlarga qarshi turish qobiliyati. Axborot xavfsizligi tahdidi ostida Buzilish, ruxsatsiz foydalanish yoki hatto vayronagarchilikka olib keladigan voqealarni yoki harakatlarni tushunish axborot manbalari boshqariladigan tizim, shuningdek dasturiy ta'minot va apparat. Axborot xavfsizligi tahdidlari ikkita asosiy turga bo'linadi -bu tabiiy va sun'iy tahdidlardir.. Tabiiy tahdidlar haqida to'xtalaylik va ularning asosiy qismini ta'kidlashga harakat qilaylik. . Tabiiy tahdidlarga Yong'inlar, toshqinlar, bo'ronlar, chaqmoq urug'lari va boshqa tabiiy ofatlar va odamlarga bog'liq bo'lmagan hodisalar mavjud. Ushbu tahdidlar orasida eng tez-tez yong'inlar. Axborot xavfsizligini ta'minlash, bu tizim elementlari (raqamli ma'lumotlar tashuvchilar, serverlar, arxivlar va boshqalar), yong'in xavfsizligi va yong'inni o'chirish uchun mas'ul bo'lgan binolarning jihozidir. Ushbu barcha qoidalarga rioya qilish, olovdan ma'lumot yo'qolishiga tahdidni minimallashtirishga imkon beradi. Agar media tashuvchilar bilan xonalar suv omborlariga yaqin joyda joylashgan bo'lsa, ular suv toshqini tufayli axborotni yo'qotish xavfi ostida. Bunday vaziyatda amalga oshirilishi mumkin bo'lgan

yagona narsa, xuddi shu binoning birinchi qavatlarida, toshqinga moyil bo'lgan binoning birinchi qavatlarida vositalarni saqlashni bartaraf etishdir. Boshqa tabiiy tahdid -bu fermuar. Ko'pincha, chaqmoqni puflaganda juda tez-tez tarmoq kartalariElektr podstansiyalari va boshqa qurilmalar. Ketishda, ayniqsa sezilarli yo'qotishlar tarmoq uskunalari Banklar kabi yirik tashkilotlar va korxonalar amalga oshirilmoqda. Oldini olish uchun shunga o'xshash muammolar Ulanish tarmoqlari kabellari saqlangan (himoyalangan) tarmoq kabeli Elektromagnit aralashishga chidamli va kabel ekranida ekranga olib borilishi kerak. Elektr podstansiyalarini elektr podstansiyalarini kiritish uchun chaqmoqni oldini olish uchun siz erga o'rnatilgan rampani o'rnatishingiz kerak va kompyuterlar va serverlar uzluksiz quvvat manbalari bilan jihozlangan. Tahdidlarning quyidagicha qarashlari sun'iy tahdidlarkim o'z navbatida ular bexosdan va qasddan tahdidlarga bo'lingan. Vaqtinchalik tahdidlar -Odamlar beparvolik, johillik, sezish yoki qiziquvchanlik tufayli harakat qiladigan harakatlar. Bunday tahdidlarning bunday turiga o'rnatish kiradi dasturiy mahsulotlarish uchun zarur bo'lgan ro'yxatga kiritilmagan va keyinchalik tizimning beqaror ishlashiga va ma'lumotlarning yo'qolishiga olib kelishi mumkin. Bu shuningdek, yovuz niyat bo'lmagan boshqa "tajribalar", va ularni topshirgan odamlar oqibatlarini anglamadilar. Afsuski, bunday tahdidlarning bu turi nafaqat xodimlar malakali, balki har bir kishi ruxsatsiz harakatlarida ro'y beradigan xavfni xabardor qilishlari lozimdir. Qasddan tahdidlar -qasddan jismoniy halokatning yomon maqsadi bilan bog'liq tahdidlar, keyinchalik tizimning ishlamaydi. Ichki va tashqi hujumlar qasddan tahdidlarni o'z ichiga oladi. Mashhur e'tiqodga zid, yirik kompaniyalar ko'p millionli yo'qotishlarni amalga oshiradilar, ko'pincha xaker hujumlaridan emas, balki o'z xodimlarining aybi bilan. Zamonaviy hikoyalar ma'lumotlarning qasddan ichki tahdidlariga ko'p misollarni biladi -bu raqibni keyingi qismlarga yoki firmadagi ish haqiyoki holatidan norozi bo'lgan qasoskorlar, qasos oluvchi xodimlar. . Bunday holatlar minimal bo'lishi uchun minimal bo'lishi uchun tashkilotning har bir xodimi, "Ishonchlilik holati" deb atashlari kerak. Tashqi Tahdidlar xaker hujumlarining tahdidlari bilan bog'liq bo'lishi mumkin. Agar axborot tizimi global Internet tarmog'i bilan bog'liq bo'lsa, unda xaker hujumlarining oldini olish uchun siz asbob-uskunalar va amalga oshirilgan dasturiy

ta'minot qurilishi mumkin bo'lgan xavfsizlik devoridan (xavfsizlik devori) foydalanishingiz kerak. Axborot tizimining ishini buzishga yoki ma'lumotlarga ruxsatsiz kirish huquqini olish uchun shaxs xaker va ba'zan "kompyuter qaroqchisi" deb nomlanadi. Boshqa qismlarni o'zlashtirishga qaratilgan noqonuniy xatti-harakatlarida, xakerlar ularga eng ishonchli ma'lumotlarni beradigan maxfiy ma'lumotlarni topishga intilishadi maksimal hajmi dan minimal narx uning kvitansiyasida. Turli xil fokuslar va ko'plab texnikalar va vositalar, bunday manbalarga yo'llar va yondashuvlar tanlanadi. Bunday holda, axborot manbai, tajovuzkorlarga yoki raqobatchilarga alohida qiziqish uyg'otadigan muayyan ma'lumotlarga ega moddiy ob'ektni anglatadi. Axborot xavfsizligiga va ACning normal ishlashi uchun asosiy tahdidlar: Maxfiy ma'lumotlar oqishi; Ma'lumotni buzish; Axborot resurslaridan ruxsatsiz foydalanish; Axborot resurslaridan noto'g'ri foydalanish; Abonentlar o'rtasida ruxsatsiz ma'lumot almashish; Axborotni rad etish; Buzish axborot xizmati; Imtiyozlardan noqonuniy foydalanish. Maxfiy ma'lumotlarning oqishi -Maxfiy ma'lumotning IC yoki Xizmatga ishonib topshirilgan yoki ish paytida ma'lum bo'lgan shaxslar doirasidan tashqarida nazoratsiz chiqishdir. Bu oqish natijasi bo'lishi mumkin: Maxfiy ma'lumotlarni oshkor qilish; Turli xil, asosan texnik,kanallar haqida ma'lumot berish; Maxfiy ma'lumotlarga ruxsatsiz kirish turli xil usullar. Egasining egasi yoki egasi tomonidan oshkor qilish, mansabdor shaxslarning qasddan yoki ehtiyot bo'lmagan harakatlari va tegishli ma'lumotlardan foydalanuvchilar o'rnatilgan usul Ularga xizmat yoki ish uchun ushbu ma'lumotga ruxsat berilmagan bilan tanishishga olib keldi. Vizual-optik, akustik, elektromagnitva boshqa kanallar bo'yicha maxfiy ma'lumotlarni saqlab qolish mavjud. Ruxsatsiz kirish -Maxfiylik bilan himoyalangan ma'lumotlarga ega bo'lmagan shaxs tomonidan maxfiy ma'lumotlarni noqonuniy ravishda istisno qilish. Ma'lumotlarga ruxsatsiz kirishning eng keng tarqalgan yo'llari quyidagilardan iborat: Elektron nurlanishni ushlash; Jozibadorlar (xatcho'plar) dan foydalanish (xatcho'plar); Masofaviy fotosurat; Akustik nurlanishni ushlab turish va printer matnini tiklash; Mediani himoya qilish choralari bilan nusxa ko'chirish Ro'yxatdan o'tgan foydalanuvchi bilan niqoblash; Tizimning so'rovlariga binoan niqoblash; Dasturiy tuzoqlardan foydalanish; Dasturlash tillar va operatsion tizimlarning kamchiliklaridan foydalanish; Maxsus ishlab

chiqilgan apparatning uskunalari va aloqa liniyalariga noqonuniy ulanish, axborot olish imkoniyatini beradigan darajada foydalanish; Zararli xulosalar himoya mexanizmlari tufayli; Shifrlangan maxsus dasturlar bo'yicha shifrlash: ma'lumot; Axborot infektsiyalari.Ro'yxatga olingan kirish yo'llari etarli darajada yirik texnik bilim va tegishli apparat yoki dasturiy ta'minot ishlanmalarini talab qiladi. Masalan, texnik oqish kanallaridan foydalanish Axborotnoma manbashiga ta'sir qiluvchi ma'lumotni himoya qiladigan tajovuzkorga nisbatan jismoniy usullardan iborat. Oqilona kanallarning paydo bo'lishining sababi -konstruktiv va texnologik nomukammallikdir solutionlarni hal qilish yoki operatsion elementlar yordamida. Bularning barchasi xakerlarga ma'lum bir maqsadli yaratishga imkon beradi jismoniy printsiplar Ushbu printsiplarga xos bo'lgan ma'lumotni tashkil etuvchi transduserlar -oqish kanali. Biroq, ruxsatsiz kirishning asosiy usullari etarli: Axborot tashuvchilari va hujjatli chiqindilarini o'zlashtirish; Tashshi bilan hamkorlik; Krakerdan hamkorlik qilish; Tushirish; Tinglash; Kuzatish va boshqa usullar. Maxfiy ma'lumotlarning oqishi usullari va uning foydalanuvchilari faoliyat ko'rsatadigan tashkilot uchun muhim moddiy va ma'naviy zararlarga olib kelishi mumkin. U erda katta to'plam mavjud zararli dasturlarMa'lumotlar bazasidagi va kompyuterlarda ma'lumotlarning maqsadi. Ushbu dasturlarning ko'p sonli turlari ulardan himoya qilish va ishonchli himoya vositalarini rivojlantirishga imkon bermaydi. Politsiyaga bo'lgan barcha potentsial xavfsizlikka tahdidlarni 2 ta asosiy sinfga bo'lish mumkin.Art Hujumchilar tomonidan qasddan qilingan harakatlar bilan bog'liq bo'lmagan tahdidlar va chaqirilgan tasodifiy daqiqalarda amalga oshiriladi tasodifiy yoki bexosdan. Umuman olganda tasodifiy tahdidlarni amalga oshirish mexanizmi juda yaxshi o'rganilgan, bu tahdidlarga qarshi katta tajriba to'plangan. Tabiiy ofatlar va baxtsiz hodisalar Biroq politsiya uchun eng halokatli oqibatlar, ikkinchisi jismoniy halokatga duchor bo'lganligi sababli, ma'lumot yo'qoladi yoki unga kirish imkonsiz bo'ladi. Ishlatmalar va muvaffaqiyatsizliklar Kompleks tizimlar muqarrar. Muvaffaqiyatsizlik va muvaffaqiyatsizliklar natijasida texnik vositalarning faoliyati buzilgan, ma'lumotlar va dasturlar va dasturlar yo'q qilinadi va buzilgan, qurilmaning ishlash algoritmi buzilgan. Politsiya, algoritmik va dasturiy ta'minotni rivojlantirishda xatolar Xatolar etishmovchiligining oqibatlari va texnik vositalarni rad

etish oqibatlariga bog'liq xatolarga olib keladi. Bundan tashqari, bunday xatolar politsiya resurslariga ta'sir qilish uchun tajovuzkorlar tomonidan ishlatilishi mumkin. Natijada foydalanuvchi xatolari va xizmat ko'rsatish xodimlari Xavfsizlik buzilishi 65% hollarda sodir bo'ladi. Xodimlar tomonidan funktsional majburiyatlarni e'tiborsiz, beparvo yoki diqqatli bo'lmagan holda bajarish, ma'lumotlarning yaxlitligi va maxfiyligini buzishga olib keladi.

Xulosa

Online platformalarda savdo qilmoqchi bo’lsangiz yoki o’zingizning shaxsiy tovarlaringizni sotib yuborguncha yoki sotib olguncha shaxsiy ma’lumotlaringizni, karta raqamlaringizni, oila a’zolaringizni ma’lumotlarini tarqatmang.

Foydalanilgan adabiyotlar:

1. www.unicon.uz
2. www.intuit.ru
3. cryptography.ru
4. https://csec.uz/uz/