KIBERXAVFSIZLIK: ZAMONAVIY XAVFLAR VA SHAXSIY MA'LUMOTLARNI HIMOYA QILISH USULLARI.

Qurbanov Shuxrat Uskanovich
Mudofaa vazirligi harbiy hizmatchisi

Annotatsiya: *Ushbu maqola zamonaviy kiberxavfsizlik masalalarini, jumladan, fishing hujumlari, zararli dasturlar, DDoS hujumlari va ijtimoiy muhandislik texnikalarini yoritadi. Shuningdek, shaxsiy va korporativ ma'lumotlarni himoya qilish usullari, jumladan, kuchli parollardan foydalanish, ikki bosqichli autentifikatsiya, antivirus dasturlarni o‘rnatish va tizimlarni yangilash bo‘yicha tavsiyalar beriladi. Maqola nafaqat texnologik, balki ijtimoiy masalalarga ham e’tibor qaratib, kiberxavfsizlik bo‘yicha xabardorlikni oshirishni ta’kidlaydi.*

Kalit so‘zlar: *kiberxavfsizlik, fishing hujumlari, zararli dasturlar, ddos hujumlari, shaxsiy ma'lumotlarni himoya qilish, ikki bosqichli autentifikatsiya (2fa), antivirus dasturlari, tizim yangilanishi, ijtimoiy muhandislik, ma'lumotlar zaxirasi.*

Kiberxavfsizlik bugungi kunda har qachongidan ham dolzarb masalaga aylangan. Axborot texnologiyalari rivojlanishi bilan bir qatorda, kiberjinoyatlar ham kengayib bormoqda. Shaxsiy va korporativ ma'lumotlarni himoya qilish, ijtimoiy tarmoqlardagi faoliyat xavfsizligini ta'minlash har bir inson va tashkilot uchun muhimdir. Ushbu maqolada zamonaviy xavflar va ularga qarshi kurashish usullari haqida so‘z yuritamiz.

Zamonaviy xavflar.

Kiberjinoyatlar turli shakllarda namoyon bo‘lmoqda, ularning ayrimlari quyidagilardan iborat:

Fishing hujumlari.

Fishing (phishing) – bu kiberhujumlarning keng tarqalgan shakli bo‘lib, unda firibgarlar soxta elektron pochta xabarlari, veb-saytlar yoki boshqa ko‘rinishdagi kommunikatsion vositalar orqali shaxsiy ma’lumotlarni qo‘lga kiritishga harakat qilishadi. Bu turdagi hujumlar odatda foydalanuvchilarning parollari, kredit yoki debit karta ma’lumotlari, bank hisoblari haqidagi maxfiy ma’lumotlar, ijtimoiy tarmoqlarga kirish ma’lumotlari yoki boshqa qimmatli va shaxsiy ma’lumotlarni nishonga oladi. Fishing xurujlarida firibgarlar o‘zlarini qonuniy tashkilotlar, masalan, banklar, davlat idoralari yoki yirik kompaniyalar vakili sifatida ko‘rsatishga harakat qilishadi. Ular foydalanuvchilarga real tashkilotlardan kelgan kabi ko‘rinadigan soxta xabarlarni yuborib, odatda xavf tug‘ilganini ko‘rsatishga yoki muhim harakatni amalga oshirishga undaydi. Masalan, foydalanuvchi hisobining to‘xtatilganini, firibgarlik faoliyati aniqlanganini yoki shartnoma shartlari yangilangani haqida bildirishlar yuborish orqali ularni o‘z ma’lumotlarini kiritishga jalb qilishadi. Soxta xabarlar ko‘pincha haqiqiy manbalar ko‘rinishini berish uchun rasmiy logotiplar, professional tilda yozilgan matnlar va boshqa ishonaverli

elementlardan foydalanadi. Shu bilan birga, ularda ko‘pincha foydalanuvchini ma’lum bir havolaga o‘tishga, hujjatlarni yuklab olishga yoki dasturiy ta’minotni o‘rnatishga undovchi so‘rovlar mavjud bo‘ladi. Ushbu havolalar odatda firibgarlarning boshqaruvidagi veb-saytlarga olib boradi, bu esa foydalanuvchining shaxsiy ma’lumotlarini kiritishiga olib keladi.

Zararli dasturlar (malware).

Zararli dasturlar (malware) – bu maxsus yaratilgan dasturiy ta’minot bo‘lib, uning asosiy maqsadi kompyuter tizimlariga zarar yetkazish, shaxsiy ma’lumotlarni o‘g‘irlash yoki foydalanuvchining resurslarini noqonuniy ravishda ishlatishdan iborat. Ushbu dasturlar kiberjinoyatchilar tomonidan foydalanuvchilarga yoki tashkilotlarga zarar yetkazish uchun qo‘llaniladi va ular turli shakllarda mavjud. Zararli dasturlarning eng keng tarqalgan shakllaridan biri viruslar bo‘lib, ular o‘zlarini boshqa dasturlar yoki fayllarga biriktiradi va tizimda keng tarqaladi. Viruslar kompyuterlarning ish faoliyatini buzishi, ma’lumotlarni yo‘q qilishi yoki o‘zgartirishi mumkin. Troyan dasturlari esa foydalanuvchilarga foydali yoki zararsiz dastur sifatida ko‘rinadi, ammo aslida tizimga zarar yetkazuvchi yashirin funktsiyalarni bajaradi, masalan, orqa eshik orqali tizimga ruxsatsiz kirish imkonini beradi. Bundan tashqari, ransomware kabi zararli dasturlar ham keng tarqalgan bo‘lib, ular foydalanuvchining ma’lumotlarini shifrlab qo‘yadi va ularni qayta tiklash uchun pul talab qiladi. Ushbu dastur odatda korxonalar va tashkilotlarni nishonga olsa-da, oddiy foydalanuvchilar ham zarar ko‘rishi mumkin. Yana bir tur – spyware bo‘lib, u foydalanuvchining faoliyatini yashirincha kuzatadi va ma’lumotlarini yig‘adi. Masalan, klaviatura orqali kiritilgan parol va boshqa shaxsiy ma’lumotlarni o‘g‘irlashga qodir. Zararli dasturlar tizim xavfsizligini buzib, nafaqat shaxsiy ma’lumotlarning o‘g‘irlanishiga olib keladi, balki foydalanuvchining ish faoliyatini to‘xtatib qo‘yishi, moliyaviy yo‘qotishlarga sabab bo‘lishi va boshqa jiddiy zararlar yetkazishi mumkin. Ulardan himoyalanish uchun antivirus dasturlaridan foydalanish, tizimni muntazam ravishda yangilash, shubhali havolalar va fayllardan ehtiyot bo‘lish, shuningdek, kiberxavfsizlik bo‘yicha ehtiyot choralariga rioya qilish muhimdir.

DDoS hujumlari.

DDoS (Distributed Denial of Service) hujumlari – bu kiberjinoyatchilar tomonidan maqsadli tizim yoki xizmatni ishlamay qolishiga yoki sezilarli darajada sekinlashishiga olib kelish uchun amalga oshiriladigan hujumlardir. Ushbu hujumlar tizimga bir vaqtning o‘zida ko‘plab so‘rovlar yuborish orqali uning resurslarini haddan tashqari yuklash va odatiy foydalanuvchilar uchun xizmatni mavjud bo‘lmasligini ta’minlashni maqsad qiladi. DDoS hujumlari ko‘pincha "botnet" deb ataluvchi zararli qurilmalardan tashkil topgan tarmoq yordamida amalga oshiriladi. Botnet – bu zararli dasturlar bilan boshqarilayotgan va kiberjinoyatchilarning nazorati ostidagi kompyuterlar, serverlar yoki boshqa internetga ulangan qurilmalar yig‘indisidir. Hujum paytida botnetdan kelayotgan katta hajmdagi so‘rovlar tizimga bir vaqtda yuboriladi, natijada tizim ularga javob bera olmay qoladi va xizmat foydalanuvchilar uchun ishlamay qoladi.

Ma'lumotlarning buzilishi (data breach).

Ma'lumotlarning buzilishi (data breach) – bu tashkilotlar yoki shaxsiy shaxslarning ma'lumotlar bazasiga noqonuniy kirish orqali shaxsiy, moliyaviy yoki boshqa muhim ma’lumotlarning o‘g‘irlanishi yoki buzilishi holatidir. Bu holat ko‘pincha kiberjinoyatchilar tomonidan amalga oshiriladi, ular tashkilotlarning ma'lumotlar bazasini nishonga olib, ulardagi shaxsiy yoki moliyaviy ma'lumotlarni qo‘lga kiritishadi. Ma'lumotlarning buzilishi natijasida, foydalanuvchilar yoki tashkilotlarning shaxsiy ma'lumotlari, kredit karta raqamlari, parollar yoki boshqa maxfiy ma'lumotlari noqonuniy qo‘llarga o‘tishi mumkin. Ma'lumotlarning buzilishi turli usullar bilan amalga oshirilishi mumkin. Eng keng tarqalgan usullardan biri phishing hujumlari bo‘lib, unda kiberjinoyatchilar soxta xabarlar yoki veb-saytlar orqali foydalanuvchilarning shaxsiy ma’lumotlarini o‘g‘irlaydilar. Boshqa usullar esa malware (zararli dasturlar) yoki SQL injection (ma'lumotlar bazasiga zararli kod kiritish) orqali tizimlarga kirish va ularning xavfsizlik choralari buzilishi hisoblanadi. Ma'lumotlar buzilishi tashkilotlar uchun jiddiy oqibatlarga olib kelishi mumkin. Bu hujumlar obro‘ yo‘qotilishiga, moliyaviy zarar yetkazilishiga va qonuniy javobgarlikni keltirib chiqarishi mumkin. Shaxsiy foydalanuvchilar uchun esa kredit kartalari, ijtimoiy tarmoqlardagi akkauntlar va boshqa maxfiy ma'lumotlar o‘g‘irlanishi xavfi mavjud. Ma'lumotlarning buzilishidan himoyalanish uchun tashkilotlar va foydalanuvchilar kuchli xavfsizlik choralari ko‘rishlari kerak. Bunga kriptografiya, kuchli parollarni ishlatish, ikki faktorli autentifikatsiya (2FA), doimiy tizim yangilanishlari va antivirus dasturlari yordamida xavfsizlikni ta'minlash kiradi.

Shaxsiy ma’lumotlarni himoya qilish usullari.

Shaxsiy ma'lumotlarni himoya qilish uchun quyidagi amaliy tavsiyalarni bajarish muhimdir:

Kuchli parollarni ishlatish. Parollaringiz kamida 12 ta belgidan iborat bo‘lib, katta va kichik harflar, sonlar hamda maxsus belgilarni o‘z ichiga olishi lozim. Har bir xizmat uchun alohida parol yarating.

Ikki bosqichli autentifikatsiya (2FA). Ikki bosqichli autentifikatsiya tizimlari orqali shaxsiy akkauntlaringiz xavfsizligini oshiring. Ushbu tizim paroldan tashqari qo‘shimcha xavfsizlik kodini talab qiladi.

Antivirus va xavfsizlik dasturlaridan foydalanish. Kompyuter va mobil qurilmalar uchun ishonchli antivirus dasturlarini o‘rnatib, ularni muntazam yangilab turing.

Ijtimoiy tarmoqlarda ehtiyot bo‘lish. Shaxsiy ma’lumotlaringizni ijtimoiy tarmoqlarda oshkor qilmang. Profilingizni faqat do‘stlaringizga ko‘rinadigan qilib sozlang.

Soxta xabar va veb-saytlardan ehtiyot bo‘ling. Fishing hujumlaridan himoyalanish uchun noma’lum manbalardan kelgan havolalarni ochmang va soxta xabarlar orqali yuborilgan ilovalarga ishonmang.

Vaqti-vaqti bilan ma'lumotlarni zaxiralash. Muhim fayllaringizni muntazam ravishda tashqi qurilmalarga yoki bulut xizmatlariga zaxiralang.

Tizimlarni yangilab turing. Operatsion tizim va dasturlarni muntazam ravishda yangilash orqali xavfsizlikni oshiring. Yangilanishlar odatda xavfsizlik zaifliklarini bartaraf etadi.

Tashkilotlar uchun tavsiyalar.

Korxonalar o‘z ma’lumotlarini himoya qilish uchun quyidagi choralarni ko‘rishlari lozim:

1. Xodimlarni kiberxavfsizlik bo‘yicha muntazam o‘qitish va ularning xabardorligini oshirish.
2. Ma’lumotlarni shifrlash texnologiyalaridan foydalanish.
3. Zaxira nusxa olish va halokatga qarshi tiklanish rejalarini ishlab chiqish.
4. Xavfsizlik devorlarini (firewall) va kiberxavfsizlik monitoringi tizimlarini joriy qilish.

Xulosa:

Kiberxavfsizlik nafaqat texnologik muammo, balki ijtimoiy masala hamdir. Shaxsiy va tashkilot darajasida xavfsizlik choralarini ko‘rish, zamonaviy xavflar haqida xabardorlikni oshirish orqali o‘zimizni va ma’lumotlarimizni himoya qilishimiz mumkin. Texnologiyadan xavfsiz foydalanishni o‘rganish, bu boradagi bilim va ko‘nikmalarni oshirish bugungi kunda har birimizning asosiy vazifamiz bo‘lib qolmoqda.

FOYDALANILGAN ADABIYOTLAR:

1. https://cyberleninka.ru/article/n/kiber-xavfsizlik-muammolari-va-uni-ta-minlash-usullari
2. https://cyberleninka.ru/article/n/ma-lumotlar-xavfsizligini-himoya-qilish-usullari-va-tahlilima-lumotlar-xavfsizligini-himoya-qilish-usullari-va-tahlili
3. https://uzbekdevs.uz/maqolalar/kiberxavfsizlik-zamonaviy-dunyoning-asosiy-muhofazasi-hackzone