KIBERXAVSIZLIK ASOSLARI

Zavqiyev Suxrob Sunnatullo o'g'li

Muhammad al Xorazmiy nomidagi Toshkent axborot texnologiyalari Universiteti
Kiberxavfsizlik fakulteti Axborod xavfsizligi yonalishi 3-bosqich Talabalari

Annotatsiya: Ushbu maqolada kiberxavfsizlik asoslari keng qamrovda yoritilgan. Axborotni himoya qilish, tizimlar va tarmoqlar xavfsizligi, kriptografiya, hamda foydalanuvchilar xavfsizligi kabi muhim yo'nalishlar batafsil tahlil qilingan. Shuningdek, zamonaviy kiberxavfsizlik tahdidlari — xakerlik hujumlari, zararli dasturlar, phishing va DDoS kabi tahdidlar misollar bilan tushuntirilgan. Maqolada kiberxavfsizlikni ta'minlash uchun amaliy choralar, jumladan kuchli parollar, ikki bosqichli autentifikatsiya, antivirus va dasturiy ta'minotni yangilash muhimligi ta'kidlangan. Foydalanuvchining kiberxavfsizlikda tutgan roli va mas'uliyati ham alohida ko'rib chiqilgan. Maqola zamonaviy raqamli muhitda xavfsizlikni ta'minlashga oid muhim tavsiyalar beradi.

Kalit so'zlar: Kiberxavfsizlik, Axborotni himoya qilish, Kriptografiya, Xakerlik hujumlari, Zararli dasturlar (Malware), Phishing, DDoS hujumlari, Parollar xavfsizligi, Ikki bosqichli autentifikatsiya, Foydalanuvchi xavfsizligi

KIRISH

Raqamli texnologiyalarning jadal rivojlanishi inson hayotining deyarli barcha jabhalariga ta'sir ko'rsatmoqda. Axborot texnologiyalari kundalik hayotimizning ajralmas qismiga aylangan bir davrda, axborotning xavfsizligi masalasi ham dolzarb tus olmoqda. Bugungi kunda nafaqat davlatlar, balki yirik kompaniyalar, tashkilotlar va oddiy foydalanuvchilar ham kiberxavfsizlik tahdidlariga duch kelmoqda.

Kiberxavfsizlik — bu raqamli axborot va tizimlarni ruxsatsiz kirish, o'g'irlash, o'zgartirish yoki yo'q qilishdan himoya qilishga qaratilgan chora-tadbirlar majmuasidir. U nafaqat texnik muammolarni hal qiladi, balki ijtimoiy, iqtisodiy va siyosiy barqarorlikni ham ta'minlashda muhim rol o'ynaydi. Xususan, bank tizimlaridan tortib sog'liqni saqlash, ta'lim va davlat boshqaruvigacha bo'lgan sohalarda kiberxavfsizlik muammolari tobora kuchayib bormoqda.

Shunday ekan, har bir foydalanuvchi va mutaxassis uchun kiberxavfsizlikning asosiy tushunchalari va tamoyillarini bilish — zamonaviy hayot talabi hisoblanadi. Quyida biz kiberxavfsizlikning muhim yo'nalishlari, xavf-xatarlar va ularga qarshi samarali choralar haqida so'z yuritamiz.

Kiberxavfsizlikning asosiy yo'nalishlari

Bugungi kunda raqamli dunyo kundan-kunga murakkablashib bormoqda. Shu bilan birga, kiberxavfsizlikning muhimligi ham ortib bormoqda. Kiberxavfsizlik nafaqat texnik mutaxassislar, balki oddiy foydalanuvchilar uchun ham o'z ahamiyatini tobora oshirmoqda. Quyida kiberxavfsizlikning asosiy yo'nalishlarini batafsilroq ko'rib chiqamiz.

Axborotni himoya qilish Axborot bugungi kunda eng qimmatbaho resurslardan biri hisoblanadi. Masalan, bank hisobingizdagi pul miqdori, shaxsiy ma'lumotlaringiz yoki kompaniyangizning sirli hujjatlari — bularning barchasi axborotdir. Agar bu axborot yomon niyatli shaxslar qo'liga tushsa, katta zarar yetishi mumkin.

Axborotni himoya qilish deganda, uni ruxsatsiz kirishdan, o‘g‘irlashdan, buzishdan va yo‘q qilishdan saqlash tushuniladi. Bu uch asosiy tamoyilga asoslanadi:

- **Maxfiylik:** Masalan, sizning shaxsiy elektron pochtaingizni faqat siz va ishonchli shaxslar ko‘ra olishi kerak.
- **Butunlik:** Axborot buzilmagan, o‘zgartirilmagan holda saqlanishi kerak. Agar kimdir sizning bank hisobingizdagi raqamlarni o‘zgartirsa, bu butunlik buzilishi hisoblanadi.
- **Mavjudlik:** Axborot kerak bo‘lgan vaqtda ochiq va foydalanishga tayyor bo‘lishi muhim. Masalan, tibbiyot tizimida bemorning ma’lumotlari doimo tezkor va mavjud bo‘lishi kerak.

Tizimlar va tarmoqlar xavfsizligi Internet orqali bog‘langan kompyuterlar va serverlar tarmoqlarni tashkil qiladi. Har kuni minglab xakerlar va zararli dasturlar ushbu tarmoqlarga hujum qilishga urinadi. Tarmoqlar xavfsizligini ta’minlash — bu ular orqali axborotning ruxsatsiz ko‘chirilishini va buzilishini oldini olishdir.

Misol uchun, **firewall** (xavfsizlik devori) — bu kompyuter tarmoqlarini himoya qiluvchi devor kabi ishlaydigan dastur yoki qurilma. U ruxsatsiz kirishni bloklaydi va faqat ishonchli trafikni o‘tkazadi. Shuningdek, **DDoS hujumlar** — bu tarmoq resurslarini ko‘p miqdordagi so‘rovlar bilan to‘ldirib, ularni ishlashga yaroqsiz qilish usuli hisoblanadi. Bunday hujumlarga qarshi maxsus dasturiy vositalar va strategiyalar mavjud.

Kriptografiya asoslari Kriptografiya — axborotni sir saqlash san’ati va fanidir. Bu soha ma’lumotlarni maxfiy holda yuborish va saqlash uchun ishlatiladi. Kriptografiya usullari orqali yuborilayotgan xabar yoki ma’lumot faqat maxsus kalitga ega bo‘lgan shaxs tomonidan o‘qilishi mumkin.

Misol uchun, siz do‘stingizga sirli xabar yubormoqchisiz, ammo bu xabar yo‘l davomida boshqa birov tomonidan o‘qilmasin. Kriptografiya yordamida bu xabar shifrlanadi (kodlanadi) va faqat do‘stingiz uni maxsus kalit yordamida yechadi. Internetda bank operatsiyalarining xavfsizligi, elektron pochtaning himoyasi, va hatto telegram va whatsapp kabi messenjerlarning shifrlangan chatlari — bularning barchasi kriptografiyaga asoslanadi.

Foydalanuvchi xavfsizligi Kiberxavfsizlikning eng muhim va eng zaif bo‘g‘inlaridan biri — foydalanuvchilar. Hatto eng kuchli tizim ham, agar foydalanuvchi parolini oson taxmin qilsa yoki shubhali havolani bosib qo‘ysa, buzilishi mumkin.

Misol uchun, ko‘pchilik odamlar parollarini "123456" yoki "password" kabi oddiy so‘zlardan tanlaydi. Bu juda xavfli. Shuningdek, ko‘plab foydalanuvchilar phishing (firibgarlik) xatlariga aldanib, o‘z shaxsiy ma’lumotlarini begonalarga berib qo‘yadi. Masalan, ular bank yoki davlat tashkilotidan kelgan deb o‘ylagan soxta xatga javob berib, hisob raqamlarini yo‘qotib qo‘yishadi.

Shuning uchun foydalanuvchilar:

- Kuchli va murakkab parollarni tanlashlari,
- Parollarni muntazam yangilab turishlari,
- Shubhali link va xatlar bilan ehtiyotkorlik bilan munosabatda bo‘lishlari,
- Ikki bosqichli autentifikatsiya (2FA)ni yoqishlari kerak.

Mana shu asosiy yo‘nalishlar kiberxavfsizlikning poydevorini tashkil qiladi va zamonaviy raqamli dunyoda himoyaning ajralmas qismidir. Har bir yo‘nalish o‘ziga xos murakkabliklarga ega va ularni yaxshi tushunish har birimizning raqamli hayotimizni xavfsizroq qilishga yordam beradi.

Kiberxavfsizlik tahdidlari va ularning turlari

Kiberxavfsizlikning asosiy maqsadi — axborot va tizimlarni himoya qilish. Biroq, har kuni minglab yangi tahdidlar paydo bo‘lib, texnologiyalarni sinovdan o‘tkazmoqda. Keling, eng keng tarqalgan va xavfli tahdid turlarini ko‘rib chiqamiz.

Xakerlik hujumlari Xakerlar — bu turli sabablarga ko‘ra kompyuter tizimlariga ruxsatsiz kirishga harakat qiladigan shaxslar. Ularning maqsadi ma’lumotlarni o‘g‘irlash, buzish yoki zarar yetkazish bo‘lishi mumkin. Misol uchun, 2017-yilda yuz bergan “WannaCry” ransomware hujumi butun dunyo bo‘ylab yuz minglab kompyuterlarni qulflab, ulardan pul talab qilgan edi. Ushbu hujum natijasida ko‘plab yirik kompaniyalar va davlat tashkilotlari jiddiy zarar ko‘rdi.

Zararli dasturlar (Malware) Malware — bu zarar yetkazish uchun yaratilgan dasturlar to‘plamidir. Ular orasida viruslar, trojanlar, ransomware (pul talab qiluvchi dasturlar), spyware (shaxsiy ma’lumotlarni yig‘uvchi dasturlar) va boshqalar bor. Masalan, viruslar kompyuteringizdagi fayllarni yo‘q qilishi yoki buzishi mumkin.

Fishing (Phishing) Fishing — bu ijtimoiy muhandislik usuli bo‘lib, unda firibgarlar sizni aldab, maxfiy ma’lumotlaringizni olishga harakat qiladi. Misol uchun, sizga bank nomidan yuborilgan soxta SMS yoki email keladi va unda parolingizni yoki kartangiz raqamini kiritishingiz so‘raladi. Ko‘pchilik bunday xabarlarga ishonib, ma’lumotlarini yo‘qotadi.

DDoS hujumlar DDoS (Distributed Denial of Service) hujumlarida internet resursiga ko‘p sonli so‘rovlar yuborilib, u ishini to‘xtatadi yoki juda sekin ishlaydi. Bu hujumlar orqali vebsaytlar yoki onlayn xizmatlar vaqtincha ishlamay qoladi. Masalan, yirik onlayn do‘kon yoki bank sayti DDoS hujum tufayli mijozlarga xizmat ko‘rsatishni to‘xtatishi mumkin.

Kiberxavfsizlikni ta’minlash choralari

Bugungi kunda kiberxavfsizlik tahdidlariga qarshi samarali kurashish uchun nafaqat kompaniyalar, balki har bir foydalanuvchi o‘zini himoya qilish choralarini bilishi va qo‘llashi zarur. Quyida kiberxavfsizlikni ta’minlashda asosiy va eng samarali choralarni sanab o‘tamiz.

Kuchli parollar va ularni boshqarish Oddiy va oson taxmin qilinadigan parollar kiberhujumchilar uchun ochiq eshikdir. Shuning uchun:

- Parollar murakkab, kamida 12 belgidan iborat bo‘lishi kerak.
- Katta va kichik harflar, raqamlar hamda maxsus belgilar qo‘shilishi lozim.
- Har bir hisob uchun alohida parol tanlash kerak, bir xil parolni bir necha joyda ishlatmaslik lozim.
- Parollarni boshqarish uchun maxsus dasturlar — password managerlardan foydalanish tavsiya etiladi.

Ikki bosqichli autentifikatsiya (2FA) 2FA — bu hisobingizga kirishda ikki xil tasdiqlashni talab qiluvchi xavfsizlik choralari tizimi. Misol uchun, parolni kiritgandan so‘ng, telefoningizga yuborilgan kodni ham kiritishingiz kerak bo‘ladi. Bu usul hisobingizni ruxsatsiz kirishdan ancha samarali himoya qiladi.

Antivirus va xavfsizlik devorlari (firewall) Kompyuteringizni virus va zararli dasturlardan himoya qilish uchun antivirus dasturlarni o‘rnatish va muntazam yangilab turish muhimdir. Shuningdek, firewall yordamida internet tarmog‘idan kelayotgan va chiqayotgan trafik nazorat qilinadi, bu esa ruxsatsiz kirishlarning oldini oladi.

Dasturiy ta’minotni muntazam yangilash Operatsion tizimlar va dasturlarni yangilab borish kiberxavfsizlik uchun juda muhimdir. Ko‘plab hujumlar dasturlardagi zaifliklardan foydalanib amalga oshiriladi. Yangilanishlar esa ushbu zaifliklarni yopadi.

Zaxira nusxalar (Backup) Muhim fayllar va ma’lumotlarning zaxira nusxalarini yaratib borish kiberhujum yoki tizim nosozligi paytida katta yordam beradi. Agar ma’lumotlar o‘g‘irlangan yoki buzilgan bo‘lsa, siz ularni qayta tiklashingiz mumkin bo‘ladi.

Xabardorlik va ta’lim Foydalanuvchilarni kiberxavfsizlik haqida muntazam o‘qitish va xabardor qilish ham juda muhim. Phishing, zararli dasturlar, ijtimoiy muhandislik kabi tahdidlar haqida bilish, ulardan himoyalanish imkonini oshiradi.

Kiberxavfsizlikda foydalanuvchining roli

Ko‘pchilik kiberxavfsizlikni faqat texnik mutaxassislar ishi deb o‘ylaydi, ammo haqiqatda eng zaif va muhim qism — bu foydalanuvchilarning o‘zi. Hatto eng ilg‘or himoya tizimlari ham, agar foydalanuvchi ehtiyotsizligi sababli zaiflik yuzaga kelsa, samara bermaydi. Shuning uchun har bir foydalanuvchi o‘z mas’uliyatini anglab, xavfsizlik choralarini qo‘llashi lozim.

Ma’suliyatli internetdan foydalanish Internetda ko‘plab firibgarliklar, zararli saytlarga havolalar va noto‘g‘ri ma’lumotlar mavjud. Foydalanuvchi har doim ehtiyotkor bo‘lishi kerak:

- Noaniq yoki shubhali manbalardan kelgan xatlarni ochmaslik,
- Tanish bo‘lmagan havolalarni bosmaslik,
- Shaxsiy ma’lumotlarni (parol, kartalar raqami, pasport ma’lumotlari) hech qachon norasmiy saytlarga kiritmaslik.

Maxfiylikni saqlash Foydalanuvchilar o‘z shaxsiy ma’lumotlarini ijtimoiy tarmoqlarda va boshqa platformalarda ortiqcha oshkor qilmasliklari kerak. Bu ma’lumotlar xakerlar tomonidan yig‘ilib, keyinchalik firibgarlikda ishlatilishi mumkin.

Parollarni doimiy yangilash va murakkab qilish Oldingi bo‘limda aytilganidek, parollarni kuchli va murakkab qilish, ularni muntazam o‘zgartirib borish foydalanuvchining asosiy vazifalaridan biridir.

Kiberxavfsizlik bo‘yicha o‘qish va xabardorlik Texnologiyalar va tahdidlar tez o‘zgarib boradi, shuning uchun foydalanuvchilar doimo yangiliklardan xabardor bo‘lishlari, kiberxavfsizlik bo‘yicha o‘qishlari, seminar va treninglarda qatnashishlari foydali.

Xulosa

Bugungi raqamli asrda kiberxavfsizlik inson hayotining ajralmas qismiga aylandi. Internet va raqamli texnologiyalar hayotimizni osonlashtirayotgani bilan birga, ular bilan bog‘liq tahdidlar ham tobora murakkablashib, xavf solmoqda. Shu bois, kiberxavfsizlik — faqat texnik mutaxassislar emas, balki har bir foydalanuvchining mas’uliyati hisoblanadi.

Maqolada ko‘rib chiqilgan asosiy yo‘nalishlar — axborotni himoya qilish, tizimlar va tarmoqlar xavfsizligi, kriptografiya, hamda foydalanuvchi xavfsizligi — raqamli dunyoda xavfsiz yashash uchun mustahkam poydevor hisoblanadi. Shu bilan birga, xakerlik hujumlari, zararli dasturlar, phishing va DDoS kabi tahdidlarni yaxshi tushunish, ularga qarshi samarali choralar qo‘llash muhimdir.

Har birimiz kuchli parollar yaratish, ikki bosqichli autentifikatsiyadan foydalanish, dasturiy ta’minotni yangilash, zaxira nusxalar yaratish hamda kiberxavfsizlik bo‘yicha muntazam o‘qib-o‘rganish orqali o‘zimizni va atrofdagilarni himoya qilishimiz mumkin.

Kiberxavfsizlikni ta’minlash — bu doimiy jarayon, unda texnologiyalar bilan birga tahdidlar ham rivojlanadi. Shuning uchun har doim hushyorlikni yo‘qotmaslik, yangi xavflar haqida xabardor bo‘lish va zarur choralarni ko‘rish muhimdir. Faqat shunday qilib, biz raqamli dunyoda ishonchli va xavfsiz harakat qilish imkoniyatiga ega bo‘lamiz.

Foydalanilgan adabiyotlar ro‘yxati:

1. **Stallings, W.** (2020). Cryptography and Network Security: Principles and Practice. Pearson Education.
— Kriptografiya va tarmoqlar xavfsizligi asoslarini tushuntiruvchi asosiy manba.

2. **Whitman, M. E., & Mattord, H. J.** (2018). Principles of Information Security. Cengage Learning.
— Axborot xavfsizligi tamoyillari va amaliy yo‘nalishlari bo‘yicha darslik.

3. **Kaspersky Lab** rasmiy veb-sayti. https://www.kaspersky.com/resource-center/threats
— Zamonaviy kiberxavfsizlik tahdidlari va ularning turlari haqida ma’lumotlar.

4. **NIST Special Publication 800-53** (2020). Security and Privacy Controls for Information Systems and Organizations.
— Axborot tizimlarini himoya qilish uchun standartlar va tavsiyalar.

5. **Symantec Corporation** (2021). Internet Security Threat Report.
— Kiberxavfsizlik sohasidagi so‘nggi tahdidlar va tahlillar.

6. **Cybersecurity & Infrastructure Security Agency (CISA)** — https://www.cisa.gov
— Kiberxavfsizlik bo‘yicha davlat resurslari va foydali tavsiyalar.