KIBERXAVFSIZLIK: ASOSIY TUSHUNCHALAR VA HIMOYA USULLARI

Eshqobilova Feruza Ikromjon qizi
O‘zbekiston davlat Jahon tillari universiteti 4- kurs talabasi

Annotatsiya: *Kiberxavfsizlik zamonaviy dunyoda har qachongidan ham dolzarb. Internet texnologiyalari rivojlanishi bilan birga kiberjinoyatlar ham ortib bormoqda. Mazkur maqolada zamonaviy tahdidlar ularning qanday xavf tug‘dirishi va ularga qarshi samarali choralari haqida batafsil ma’lumot beriladi.*

Kirish so‘zlar*: firewall, IDS/IPS dasturlari, VPN, software, task manager, windows OS, Microsoft office, adobe CC, Zero Trust, AI monitoring, Ransomware Prevention, Blockchain Security.*

KIRISH

Kiberxavfsizlik - bu kompyuter tizimlar, tarmoqlar va ma’lumotlarni kiber tahdidlardan himoya qilishga qaratilgan soha. Kiberxavfsizlikning asosiy maqsadi – ma’lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta’minlash. Kiberxavfsizlikning asosiy yo‘nalishlari tarmoq xavfsizligi, dasturiy ta’minot xavfsizligi va axborot xavfsizligi hisoblanadi.

"Tarmoq xavfsizligi – bu tarmoq orqali yuboriladigan ma'lumotlarni hackerlar, viruslar va boshqa tahdidlardan himoya qilish. Uning asosiy elementlari: firewall, IDS/IPS tizimlari va VPN hisoblanadi. Firewall tarmoqqa ruxsatsiz kirishlarning oldini oladi. Hujumlarni aniqlash va oldini olish uchun esa IDS/IPS dasturi kerak bo‘ladi. VPN - internet orqali uzatilgan ma’lumotlarni shifrlash va maxfiyligini ta’minlovchi texnologiya . Bu dastur xuddi shaxsiy tunnelga o‘xshaydi, ma'lumotlaringizni hech kim ko‘rmaydigan maxfiy yo‘l orqali yuboradi. VPN orqali kimdir sizni kuzatsa ham, ma'lumotlarni o‘qiy olmaydi."[1]

"Dasturiy ta’minot xavfsizligi - dasturlar orqali keluvchi tahdidlarga qarshi himoya. Komputerda ma’lum bir turdagi vazifani bajarish uchun ishlab chiqilgan vositadir.Aynan shu dasturiy ta’minotgina kompyuter — „quruq temir“ degan atamani yo‘qqa chiqargan. Dasturiy vositalar komputer tomonidan qo‘llaniladigan barcha dasturlar to‘plamidir. Ingiliz tilida bu atama software ya’ni „soft“ — yumshoq, „ware“ — „mahsulot“ degan ma’noni bildiradi. Shuningdek, u 3 guruhga bo‘linadi: 1-Sistema dasturlari (unga turli yordamchi vazifalarni bajaruvchi dasturlar kiradi: Task Manager (Windows OSda mavjut)), 2-Amaliy (unga foydalanuvchiga aniq bir foydalanish sohasida ma’lumotlarga ishlov berish va qayta ishlashni amalga oshiruvchi dasturlar, masalan : Microsoft Office, Adobe CC), 3-Uskunaviy dasturlar (bular dasturlash uchun ishlatiladigan dasturlar)"[2]

"Axborot xavfsizligi (inglizcha: Information Security, shuningdek, inglizcha: InfoSec) — axborotni ruxsatsiz kirish, foydalanish, oshkor qilish, buzish, o‘zgartirish,

tadqiq qilish, yozib olish yoki yo‘q qilishning oldini olish amaliyotidir.Axborot xavfsizligini ta’minlashning asosiy maqsadi ma’lumotlarning konfidensialligi, yaxlitligi va mavjudligini muvozanatli, qo‘llashning maqsadga muvofiqligini hisobga olgan holda va tashkilot faoliyatiga hech qanday zarar yetkazmasdan himoya qilishdir."[3]

Kiber tahdidlar va hujumlar turlariga fishing (phishing), DDoS hujumlari, zararli dasturlar (malware), parol o‘g‘irlash (brute-forse, dictionary attack) va h.k kiradi.

Phishing – bu xakerlarning soxta elektron pochta yoki xabarlar orqali foydalanuvchilarning login, parol yoki moliyaviy ma’lumotlarini qo‘lga kiritishga urinishidir. Bugungi kunda phishing hujumlari yanada murakkablashib, deepfake texnologiyalaridan ham foydalanilmoqda.

Oldini olish usullari:

Soxta xabarlar va havolalarni tekshirish.

Ikki bosqichli autentifikatsiyadan (2FA) foydalanish.

Email va messenjerlardagi shubhali havolalarni bosmaslik.

Ransomware (talab dasturlari) - bu hujum turi zararli dasturlar yordamida foydalanuvchining ma’lumotlarini shifrlash va ularni qayta tiklash uchun to‘lov talab qilishni o‘z ichiga oladi. Mashhur ransomware hujumlaridan biri WannaCry (2017) bo‘lib, dunyo bo‘ylab millionlab qurilmalarni zararlagan.

Himoya choralari:

Muhim ma’lumotlarni doimiy zaxiralash (backup).

Antivirus va zamonaviy EDR (Endpoint Detection and Response) tizimlaridan foydalanish.

Noma’lum dasturlarni yuklab olmaslik va ishlatmaslik.

DDoS (Distributed Denial of Service) hujumlari server yoki tarmoqni haddan tashqari yuklash orqali uning ishlashiga xalaqit beradi. Bu usul orqali kiberjinoyatchilar kompaniyalarga zarar yetkazishi yoki xizmat ko‘rsatishni vaqtincha to‘xtatishi mumkin.

Himoya choralari:

Mustahkam firewall va load balancer tizimlarini qo‘llash.

DDoS hujumlarini oldindan aniqlovchi xizmatlardan foydalanish (Cloudflare, AWS Shield).

Tarmoq monitoringi va hujum vaqtida avtomatik javob berish tizimlarini yoqish.

An’anaviy xavfsizlik yondashuvlaridan farqli o‘laroq, Zero Trust modeli har qanday foydalanuvchi yoki qurilmani shubhali deb hisoblaydi va har safar autentifikatsiya talab qiladi. Kiberxavfsizlik har kuni rivojlanib borayotgan soha bo‘lib, himoya choralari doimiy ravishda yangilanib turishi kerak. Hozirgi kunda Zero Trust, Al monitoring, Ransomware Prevention va Blockchain Security kabi texnologiyalar kiberxavfsizlikning ajralmas qismiga aylanib bormoqda.

FOYDALANILGAN ADABIYOTLAR:

1. Tarmoq xavfsizligi kirish. oktyabr 2024. [elektron manba] //ijnet.org.sayt. URL:https://learn.csclub.uz/tarmoq-xavfsizligi-1/tarmoq-xavfsizligi-kirish (murojaat vaqti: 15.02.2025)

2. Dasturiy ta’minot. 7-mart 2012. [elektron manba] //ijnet.org. sayt. URL:https://uz.m.wikipedia.org/wiki/Dasturiy_ta%CA%BCminot (murojaat vaqti:15.02.2025)

3. Axborot xavfsizligi. 31-iyul 2022. [elektron manba] //ijnet.org. sayt. URL:https://uz.m.wikipedia.org/wiki/Axborot_xavfsizligi# (murojaat vaqti:15.02.2025)