KIBERXAVFSIZLIK (CYBERSECURITY)

Tursunova Sevinch Tuychiboy qizi
Jizzax Yuridik texnikum informatika fani o‘qituvchisi

Annotatsiya: Ushbu maqola raqamli asrda kiberxavfsizlikning dolzarb muammolarini tahlil qiladi. Maqolada kiberhujumlarning zamonaviy turlari, ularning tizimlarga ta'siri va himoya qilishning samarali metodologiyalari ko'rib chiqiladi. Tadqiqot natijalari shuni ko'rsatadiki, texnologik yechimlar bilan bir qatorda, kiber gigiyena va inson omilini boshqarish xavfsizlik darajasini oshirishda hal qiluvchi ahamiyatga ega.

Kalit so‘zlar: kiberxavfsizlik, axborot himoyasi, kiberhujumlar, shifrlash, tarmoq xavfsizligi, ma'lumotlar maxfiyligi.

Bugungi kunda dunyo iqtisodiyoti va ijtimoiy hayoti to‘liq raqamli platformalarga bog‘liq. Biroq, texnologik taraqqiyot o‘zi bilan birga kiberjinoyatchilikning yangi va murakkab shakllarini ham olib keldi. Kiberxavfsizlik kompyuter tizimlari, tarmoqlar va ma’lumotlarni ruxsatsiz kirish, o‘zgartirish yoki yo‘q qilishdan himoya qilish san’atidir. Mazkur maqolaning maqsadi zamonaviy tahdidlar landshaftini o‘rganish va himoya tizimlarini takomillashtirish yo‘llarini tahlil qilishdan iborat.

So‘nggi yillardagi tadqiqotlar shuni ko‘rsatadiki, *fishing* (phishing) va *ransomware* (tovlamachi dasturlar) hujumlari tashkilotlar uchun eng katta xavf hisoblanadi. Xalqaro ekspertlar (masalan, NIST va ISO/IEC 27001 standartlari) himoya qilishda "mudofaaning ko‘p qatlamli yondashuvi" (Defense in Depth) muhimligini ta’kidlaydilar. Adabiyotlarda ta'kidlanishicha, eng kuchli himoya devori ham insoniy xatolik (masalan, zaif parollar) tufayli ishdan chiqishi mumkin.

Kiberxavfsizlik juda keng qamrovli soha bo‘lib, u texnologik, tashkiliy va insoniy omillarni o‘z ichiga oladi. Keling, bu mavzuni yanada chuqurroq va tizimliroq tahlil qilamiz.

Kiberxavfsizlikning "Uchburchagi" (CIA Triad)

Axborot xavfsizligining poydevori uchta asosiy tamoyilga tayanadi:

- Maxfiylik (Confidentiality): Ma’lumotlarga faqat ruxsat berilgan shaxslargina kirishini ta’minlash. (Misol: shifrlash).
- Butunlik (Integrity): Ma’lumotlarning uzatilish yoki saqlanish jarayonida ruxsatsiz o‘zgartirilmasligini ta’minlash.
- Qulaylik (Availability): Tizimlar va ma’lumotlar kerakli vaqtda foydalanuvchilar uchun ochiq bo‘lishini ta’minlash.

Kiberxavfsizlikdagi asosiy tahdidlar (Batafsil)

Ijtimoiy muhandislik (Social Engineering)

Bu texnik usul emas, balki psixologik hiyla. Hujumchi tizimni emas, insonni buzadi.

- Fishing (Phishing): Soxta bank saytlari yoki "parolingizni yangilang" mazmunidagi xatlar orqali ma’lumot o‘g‘irlash.
- Pretexting: O‘zini texnik yordam xodimi yoki bank menejeri deb tanishtirib, foydalanuvchini aldab ma’lumot olish.

Zararli dasturlar (Malware)

- Ransomware (Tovlamachilik viruslari): Kompyuterdagi barcha fayllarni shifrlab qo‘yadi va ularni ochish uchun xakerni pul (odatda kriptovalyuta) to‘lashga majbur qiladi.
- Spyware (Josus dasturlar): Sizning harakatlaringizni kuzatadi, klaviaturada nima yozayotganingizni yozib oladi (keylogger).

Texnik hujumlar

- SQL Injection: Veb-sayt ma’lumotlar bazasiga noto‘g‘ri kod yuborish orqali bazadagi barcha ma’lumotlarni o‘g‘irlash.
- Brute Force (Qo‘pol kuch): Dasturiy ta’minot yordamida millionlab parol kombinatsiyalarini avtomatik terib ko‘rish orqali hisobni buzish.

Himoya darajalari

Kiberxavfsizlikda "Chuqurlashtirilgan himoya" (Defense in Depth) tushunchasi bor. Ya’ni, bitta devorga tayanmay, bir necha qatlamli himoya o‘rnatiladi:

1. Perimetr himoyasi: Firewall (tarmog‘ingizga kiruvchi/chiquvchi trafikni nazorat qiluvchi ekran).
2. Endpoint (Qurilma) himoyasi: Antiviruslar, EDR (Endpoint Detection and Response) tizimlari.
3. Identifikatsiya: 2FA (ikki bosqichli autentifikatsiya) va MFA (ko‘p bosqichli autentifikatsiya). Hozirgi kunda eng samarali himoya hisoblanadi.
4. Zaxira nusxalash (Backup): Ma’lumotlarning tashqi xotirada yoki bulutli tizimda doimiy zaxira nusxasini saqlash (bu Ransomware hujumlarida eng katta yordamchi).

Kiberxavfsizlik mutaxassisi bo‘lish uchun yo‘l xaritasi

Agar bu sohaga jiddiy kirishmoqchi bo‘lsangiz, quyidagi bosqichlarni bosib o‘tishingiz kerak:

- Fundament:
  - Kompyuter tarmoqlari: OSI modeli, TCP/IP, DNS, DHCP, HTTP/HTTPS protokollarini tushunish.
  - OS (Operatsion tizimlar): Linux buyruqlar qatorini (terminal) mukammal o‘zlashtirish.

- Amaliy ko‘nikmalar:
  - Dasturlash: Python (kiberxavfsizlikdagi avtomatlashtirish uchun qirol), Bash, PowerShell.
  - Vulnerability Assessment: Saytlar yoki tizimlardagi zaifliklarni topish usullarini o‘rganish.
- Sertifikatlar (Xalqaro daraja):
  - *CompTIA Security+* (Boshlang‘ich daraja uchun).
  - *CEH (Certified Ethical Hacker)* (Axloqiy xakerlik).
  - *OSCP (Offensive Security Certified Professional)* (Amaliy xakerlik bo‘yicha eng nufuzli sertifikatlardan biri).

Muhim maslahat: "Zero Trust" modeliga o‘ting

Kiberxavfsizlikning zamonaviy falsafasi — "Hech kimga ishonma, har doim tekshir" (Never Trust, Always Verify). Tarmoq ichida bo‘lsangiz ham, har bir harakat, har bir kirish so‘rovi autentifikatsiya qilinishi va nazorat qilinishi kerak.

Xulosa

Munozara qilinayotgan asosiy savol shundan iboratki: kiberxavfsizlik faqat dasturiy ta'minot masalasimi yoki madaniy masala? Texnik vositalar (firewall, antivirus, IDS/IPS) zarur bo‘lsa-da, ular yagona yechim emas. Tashkilotlar o‘z xodimlarida kiber-savodxonlikni shakllantirish orqali tizimning "eng zaif halqasini" eng kuchli mudofaa qatlamiga aylantirishlari mumkin. Shuningdek, "Zero Trust" (Hech kimga ishonma) konsepsiyasi kelajakdagi xavfsizlik arxitekturasining asosi bo‘lishi kerakligi muhokama qilinmoqda.

Kiberxavfsizlik — bu tugamaydigan jarayon. Texnologiyalar rivojlangani sari tahdidlar ham evolyutsiya qiladi.

- Ko‘p faktorli autentifikatsiyani (MFA) barcha tizimlarda majburiy joriy etish.
- Doimiy ta’lim: Xodimlar uchun muntazam ravishda kiberxavfsizlik bo‘yicha treninglar o‘tkazish.
- Ma’lumotlarni zaxiralash: Muhim ma’lumotlarni oflayn yoki xavfsiz bulutli omborlarda doimiy zaxira nusxalarini saqlash.
- Monitoring: Tizimda sodir bo‘layotgan g‘ayritabiiy harakatlarni real vaqt rejimida kuzatish uchun SIEM tizimlarini joriy etish.

Foydalanilgan adabiyotlar ro‘yxati

1. Stallings, W., & Brown, L. (2018). *Computer Security: Principles and Practice* (4th ed.). Pearson. (Ushbu kitob kiberxavfsizlik asoslari va tarmoq himoyasi bo‘yicha dunyodagi eng nufuzli darsliklardan biri hisoblanadi).
2. Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems* (3rd ed.). Wiley. (Tizimli xavfsizlik va muhandislik yechimlari haqida).

3. NIST (National Institute of Standards and Technology). (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. (Kiberxavfsizlikni boshqarish bo‘yicha xalqaro standart).

4. ISO/IEC 27001:2022. *Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements*. (Axborot xavfsizligini boshqarish tizimi bo‘yicha xalqaro standart).

5. Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press. (Kiber urush va xalqaro siyosiy xavfsizlik masalalari haqida).

6. Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W. W. Norton & Company. (Ma'lumotlar maxfiyligi va kuzatuv texnologiyalari bo‘yicha).

7. Yusupov, S. S. (2023). *Axborot xavfsizligi asoslari*. Toshkent: O‘zbekiston faylasuflari milliy jamiyati nashriyoti. (O‘zbek tilidagi mahalliy darslik va manbalar).

8. Zikratov, I. A., & Zikratova, O. P. (2020). *Kiberxavfsizlik nazariyasi va amaliyoti*. (Texnik yechimlar va kriptografik himoya usullari bo‘yicha tadqiqot).