KIBERHUJUMLAR TURLARI VA ULARNING OLDINI OLISH USULLARI

TATU Fergana Branch
Xalilov Sarvarbek Anvar ugli
TATU Fergana Branch Assistant
Umarov Abdumukhtor Makhammad ugli

Abstract: *Ushbu maqolada kiberhujumlarning asosiy turlari va ularning oldini olish usullari haqida so'z yuritiladi. Maqola zamonaviy texnologik muhitda uchraydigan kiberhujumlar, ularning ishlash mexanizmlari hamda shaxsiy va korporativ xavfsizlikni ta'minlash uchun qo'llaniladigan samarali choralar haqida batafsil ma'lumot beradi. Kiberxavfsizlikka oid bu bilimlar nafaqat mutaxassislar, balki texnologiyadan foydalanuvchi har bir inson uchun muhimdir.*

Key words: *Kiberxavfsizlik, kiberhujumlar turlari, ma'lumotlarni himoya qilish, tarmoq xavfsizligi, ma'lumotlarni shifrlash, mobil qurilmalar xavfsizligi, ikki faktorli autentifikatsiya (2FA), zararli dasturlar.*

Bugungi kunda texnologiyalar har bir sohada, jumladan, kommunikatsiya, ish yuritish, sog'liqni saqlash, moliya, ta'lim va boshqa ko'plab sohalarda o'zgarmas va ajralmas qismga aylangan. Zamonaviy texnologiyalar foydalanuvchilarga o'z vaqtida va samarali xizmatlar ko'rsatish, ma'lumotlarni tezda almashish, yangi imkoniyatlarga erishish imkoniyatlarini yaratgan. Biroq, bu yuksalish bilan birga, yangi xavf-xatarlar ham paydo bo'lgan. Texnologiyalar va internetdan foydalanish ortib borishi bilan kiberhujumlar, ya'ni kompyuter tarmog'iga yoki qurilmaga nisbatan zararli harakatlar ko'paygan. Kiberhujumlar ko'plab turli shakllarda amalga oshirilishi mumkin, ulardan ayrimlari odamlarning shaxsiy ma'lumotlarini o'g'irlashga, boshqalari esa tizimlarni buzishga yoki xizmatlarni to'xtatib qo'yishga qaratilgan.

Kiberhujumlarning korxona, davlat idorasi yoki individual foydalanuvchi darajasida amalga oshirilishi mumkin. Masalan, kichik bizneslar, korporatsiyalar va davlat idoralari odatda keng tarmoq infratuzilmasiga ega bo'lib, bu esa hujumchilarga imkoniyat yaratadi. Hujumchilarning asosiy maqsadi ko'pincha foydalanuvchilarning shaxsiy yoki moliyaviy ma'lumotlarini o'g'irlash, tizimlarga zarar yetkazish yoki tashkilotlarning tarmog'ini nazorat qilish bo'ladi. Kiberhujumlar hatto davlatlar o'rtasida siyosiy, iqtisodiy va harbiy maqsadlar bilan amalga oshirilishi mumkin. Shuningdek, uy foydalanuvchilari ham bu xavflardan muhofaza qilinmagan va ko'pincha phishing xabarlar, zararli dasturlar va boshqa tahdidlar bilan duch kelishadi.

Fishing hujumlari va ularning oldini olish: Fishing kiberhujumi foydalanuvchilarning shaxsiy ma'lumotlarini o'g'irlash maqsadida soxta elektron pochta xabarlari, saytlar yoki xabarlar orqali amalga oshiriladi. Bu turdagi hujumlar odatda ishonavershilik va e'tiborsizlikdan foydalanadi. Oldini olish uchun:

Har doim elektron pochta va veb-saytlarning haqiqiyligini tekshiring, tasdiqlanmagan havolalarni bosmang, antifishing vositalaridan foydalaning.

Zararli dasturlar va ularning himoyasi: Zararli dasturlar (viruslar, trojanlar, ransomware) tizimlarga zarar yetkazish yoki ma'lumotlarni shifrlash orqali foydalanuvchilardan pul talab qilish uchun ishlatiladi. Himoya choralari quyidagilarni o'z ichiga oladi: Antivirus dasturlarni yangilangan holda saqlang, ishonchsiz dasturlarni o'rnatmang, muntazam ravishda zaxira nusxalarini yarating.

DDoS hujumlari va ularni cheklash: DDoS (Distributed Denial of Service) hujumlari tarmoqlarni haddan tashqari yuklash orqali ularni ishdan chiqaradi. Bu turdagi hujumlar korxona serverlari va veb-saytlariga katta zarar yetkazishi mumkin. Oldini olish usullari: Qo'shimcha tarmoq filtrlash vositalarini o'rnatish, tarmoq trafigini real vaqt rejimida kuzatib boorish, bulut asosidagi himoya xizmatlaridan foydalanish.

Ma’lumotlar buzilishi va uning oldini olish: Ma’lumotlar buzilishi korporativ yoki shaxsiy ma’lumotlarni noqonuniy ravishda o’g’irlash yoki buzish holatlarini anglatadi. Ushbu turdagi hujumlarga qarshi: Kuchli parollarni qo’llash va muntazam ravishda ularni yangilash, ikki faktorli autentifikatsiya (2FA) o’rnatish, ma’lumotlarni shifrlash texnologiyalaridan foydalanish muhimdir.

Ichki xodimlardan keladigan xavf-xatarlar: Ba’zan kompaniyadagi ichki xodimlar ham kiberhujum xavfini oshirishi mumkin. Ular bilmasdan zararli dasturlarni ishga tushirishi yoki ma’lumotlarni qasddan o’g’irlashi mumkin. Bunday holatlarning oldini olish uchun: Xodimlarga kiberxavfsizlik bo’yicha muntazam treninglar o’tkazing, foydalanuvchi huquqlarini cheklash, loglarni kuzatish va g’ayritabiiy faoliyatni aniqlash tizimlarini joriy eting.

Kiberhujumlarning soni va murakkabligi yildan-yilga oshib bormoqda. Foydalanuvchilar va tashkilotlar ushbu hujumlarni tushunib, ularning oldini olish choralarini ko’rishlari lozim. Samarali xavfsizlik choralari faqat texnologik vositalarni emas, balki xabardorlikni oshirish va muntazam himoya strategiyalarini qo’llashni ham o’z ichiga oladi. Faqat shunda biz kiberxavfsizlikni ta’minlashda muvaffaqiyatga erishishimiz mumkin.

FOYDALANILGAN ADABIYOTLAR

1. Muxammadovich, M. F., & Maxammad o’g’li, U. A. (2022, November). AXBOROTNI XIMOYALASH TIZIMINI ISHLAB CHIQISH. In Proceedings of International Educators Conference (Vol. 1, No. 2, pp. 187-190).

2. Умаров, А. (2023, November). ИНТЕГРИРОВАННЫЙ ПОДХОД К ПРЕПОДАВАНИЮ КРИПТОГРАФИИ И КИБЕРБЕЗОПАСНОСТИ В ВУЗАХ: ТЕОРИЯ И ПРАКТИКА. In Conference on Digital Innovation:" Modern Problems and Solutions".

3. Saminjanovna, I. G., & Maxammad o’g’li, U. A. (2024). AXBOROTNI RUXSATSIZ FOYDALANISHLARDAN HIMOYALASH. MODELS AND METHODS FOR INCREASING THE EFFICIENCY OF INNOVATIVE RESEARCH, 3(34), 366-369.

4. Умаров, А. (2023, November). ПРОЕКТНАЯ МЕТОДИКА В ПРЕПОДАВАНИИ КРИПТОГРАФИИ: РАЗВИТИЕ ТВОРЧЕСКИХ И КОММУНИКАТИВНЫХ НАВЫКОВ. In Conference on Digital Innovation:" Modern Problems and Solutions".

5. Umarov, A. (2023, November). Axborotni ruxsatsiz kirishdan himoya qilishda audit va monitoringning roli. In Conference on Digital Innovation:" Modern Problems and Solutions".

6. Umarov, A. (2023, November). Xavfsizlik hodisalari: profilaktika choralari va ma'lumotlardan ruxsatsiz foydalanishga qarshi choralar. In Conference on Digital Innovation:" Modern Problems and Solutions".

7. Mirzayev, J. B., TOJIMATOV, D. K. T. M., & KIBERHUJUMLARNI, O. O. B. Y. D. SIYOSATI YURITILISHI. ИНТЕРНАУКА Учредители: Общество с ограниченной ответственностью" Интернаука, 36-37.

8. Tojimatov, D. (2023). u KIBER TAHDIDLARNI BASHORAT QILISH VA XAVF-XATARLARDAN HIMOYALANISHDA SUN'IY INTELEKT IMKONIYATLARIDAN FOYDALANISH: DX Tojimatov. Katta o 'qituvchi, TATU Farg'ona filiali. Потомки Аль-Фаргани, 1(2), 41-44.

9. Tojimatov, D. (2023, October). VR/AR TEXNOLOGIYALARINI KIBERXAVFSIZLIK SOHASIDA QO 'LLASHNING DOLZARBLIGI. In Conference on Digital Innovation:" Modern Problems and Solutions".

10. Tojimatov, D. (2023, October). KIBERRAZVEDKA OLIB BORISH STRATEGIYASI BOSQICHLARI. In Conference on Digital Innovation:" Modern Problems and Solutions"

11. Tojimatov, D. (2023, October). KIBERRAZVEDKANI AMALGA OSHIRISHDA IJTIMOIY INJINERIYANI RO 'LI. In Conference on Digital Innovation:" Modern Problems and Solutions".

12. Tojimatov, D. X. (2023). KIBERTAHDIDLARNI OLDINI OLISHDA KIBERRAZVEDKA AMALIYOTI VA UNING USTUVOR VAZIFALARI. Al-Farg'oniy avlodlari, 1(4), 82-85.