ISSN 2181-3187

KIBERHUJUMLAR VA ULARGA QARSHI KURASHISH USULLARI

Bahramov Muhammadali Eraliyevich
Alfraganus university
bahromov1997.04.09@gmail.com

Annotatsiya

Ushbu maqola kiberxujumlarning turli xil shakllari va ularga qarshi kurashishning samarali usullarini tahlil qilishga qaratilgan. Kiberxujumlar bugungi kunda global miqyosda keng tarqalgan tahdid bo‘lib, tashkilotlar va shaxslarning shaxsiy ma'lumotlarini xavf ostiga qo‘yadi. Maqolada kiberxujumlarning asosiy turlari, masalan, phishing, DDoS hujumlari, malware (zararli dasturlar) va ransomware (malumotlarni garovga olish) kabi hujumlar tahlil qilinadi. Shuningdek, ularga qarshi kurashishning samarali strategiyalari, jumladan, xavfsizlik protokollari, kriptografiya, autentifikatsiya tizimlari, va xavfsizlik tahlili kabi usullar muhokama qilinadi. Maqola kiberxavfsizlikni ta'minlashda ilg‘or texnologiyalar va yaxshilangan siyosatlar yordamida tahdidlarga qarshi qanday samarali choralar ko‘rish mumkinligini ko‘rsatadi.

Kalit so’zlar: Kiberxujumlar, Phishing, DDoS hujumlari, Malware (zararli dasturlar), Ransomware, Kiberxavfsizlik, Xavfsizlik protokollari, Kriptografiya, Autentifikatsiya tizimlari, Xavfsizlik tahlili, Kiberhujumlarni oldini olish, Kiberxavfsizlik strategiyalari, Ma'lumotlarni himoya qilish, Kiberhujumlar va texnologiyalar, Xavfsizlik choralarini kuchaytirish.

Kiberxujumlar maqsadlari va **oqibatlari** keng va turli xil bo‘lishi mumkin. Kiberxurujchilar har xil motivlarga ega bo‘lishi mumkin, shu jumladan moliyaviy manfaatlar, siyosiy maqsadlar yoki shaxsiy manfaatlar. Quyida kiberxujumlarning asosiy maqsadlari va ularning potentsial oqibatlari haqida batafsil ma'lumot keltiraman:

Kiberhujumlar maqsadlari:

1. **Moliyaviy foyda olish:**
   - **Ransomware (Ma'lumotlarni garovga olish)**: Hujumchilar tizimga kirib, foydalanuvchining ma'lumotlarini shifrlashadi va ma'lumotlarni qaytarish uchun pul talab qilishadi.
   - **Phishing**: Soxta veb-saytlar yoki xabarlar orqali shaxsiy ma'lumotlarni, bank hisob raqamlarini, kredit kartalarini yoki boshqa moliyaviy ma'lumotlarni o‘g‘irlash.

ISSN 2181-3187

- **Kredit kartalarini o‘g‘irlash**: Hujumchilar tizimlar yoki onlayn do‘konlardan kredit karta ma'lumotlarini o‘g‘irlaydi va bu orqali pul o‘g‘irlaydi.

2. **Shaxsiy ma'lumotlarni o‘g‘irlash va maxfiylikni buzish:**
   - **Identity theft (Shaxsni o‘g‘irlash)**: Hujumchilar shaxsiy ma'lumotlarni o‘g‘irlab, ularni noto‘g‘ri ishlatishlari mumkin.
   - **Dasturlarni orqa eshiklar orqali qo‘llash**: Hujumchilar tizimga kirib, tizim ma'lumotlarini o‘g‘irlaydilar yoki foydalanuvchilarning shaxsiy axborotlarini olishadi.
3. **Tashkilotning imijini va ishonchni yo‘qotish:**
   - **Veb-saytga yoki tizimga hujum qilish**: DDoS (Distributed Denial of Service) hujumlari orqali xizmatlarni to‘xtatish, mijozlarning ishonchini yo‘qotish, kompaniyaning reputatsiyasini zararlash.
   - **Tizimlarni buzish va ma'lumotlarni shifrlash**: Ransomware hujumlari orqali tashkilotning ish faoliyatini to‘xtatish va shaxsiy ma'lumotlarni o‘g‘irlash.
4. **Siyosiy maqsadlar:**
   - **Tizimlarni sabotaj qilish**: Hujumchilar hukumat yoki siyosiy tashkilotlarga qarshi hujumlar uyushtirishi mumkin (masalan, hacktivizm, siyosiy motiovlar asosida).
   - **Propaganda tarqatish**: Hujumchilar, tizimlarni yoki ijtimoiy tarmoqlarni nazorat qilish orqali o‘z siyosiy maqsadlariga erishishga harakat qilishlari mumkin.
5. **Kompaniyaning intellektual mulkini o‘g‘irlash:**
   - **Industrial espionage (Sanoat josusligi)**: Kiberxurujchilar korxonalarning intellektual mulkini, patenti yoki noaniq texnologiyalarini o‘g‘irlaydi. Bu kompaniyalarni moliyaviy zarar ko‘rishga olib keladi.

Kiberhujumlar oqibatlari:

1. **Moliyaviy zarar:**
   - Kiberxujumlar kompaniyalarga yoki shaxsiy foydalanuvchilarga katta moliyaviy zarar yetkazishi mumkin. Misol uchun, ransomware hujumlari orqali kompaniyalar pul to‘lashga majbur bo‘lishi mumkin, yoki shaxsiy bank ma'lumotlarini o‘g‘irlagan hujumchilar pul o‘g‘irlashi mumkin.
   - Kompaniyalarga bo‘lgan zararlar nafaqat o‘g‘irlangan mablag‘lar bilan chegaralanadi, balki tizimni qayta tiklash, yangilash va xavfsizlikni kuchaytirish uchun katta xarajatlar talab etiladi.
2. **Reputatsion zarar:**

ISSN 2181-3187

- Kiberxujumlar kompaniyaning yoki shaxsning ishonchli imijini jiddiy ravishda zararlashi mumkin. Mijozlar va foydalanuvchilar tizimlarining xavfsizligi buzilganligini ko‘rganda, ular kompaniyadan uzoqlashishi mumkin.
- Xavfsizlik bo‘yicha muvaffaqiyatsizlik, brendning obro‘sini yo‘qotish va mijozlarning ishonchini yo‘qotish bilan yakunlanishi mumkin.

3. **Ma'lumotlarning yo‘qolishi yoki buzilishi:**

- Kiberxujumlar natijasida ma'lumotlar yo‘qolishi, buzilishi yoki o‘g‘irlanishi mumkin. Bu, ayniqsa, shaxsiy yoki moliyaviy ma'lumotlarni o‘g‘irlash holatlarida xavfli.
- Shifrlangan ma'lumotlarni qaytarish uchun katta xarajatlar kerak bo‘lishi mumkin, ba'zida esa ma'lumotlarni qaytarib bo‘lmaydi.

4. **Hukumat va siyosiy tizimlarga zarar:**

- Siyosiy maqsadlar bilan amalga oshirilgan kiberhujumlar hukumat tizimlariga zarar yetkazishi, davlat ma'lumotlarining o‘g‘irlanishi yoki buzilishi natijasida siyosiy beqarorlikka olib kelishi mumkin.
- Veb-saytlarga yoki onlayn tizimlarga, shu jumladan saylov tizimlariga hujumlar siyosiy muammolarni keltirib chiqarishi mumkin.

5. **Tizimlarning to‘xtashi va uzilishlar:**

- DDoS hujumlari va boshqa tizimlarga qaratilgan kiberhujumlar kompaniyalar va foydalanuvchilarning xizmatlarga kirishini to‘xtatishi mumkin. Bu, ayniqsa, tarmoq orqali ishlaydigan kompaniyalar uchun sezilarli darajada zarar keltirishi mumkin.

6. **Shaxsiy hayotning buzilishi:**

- Shaxsiy ma'lumotlar o‘g‘irlanishi, ya'ni identifikatsiya o‘g‘irlanishi (identity theft), jiddiy oqibatlarga olib kelishi mumkin. Bu odamlarning kredit reytingini buzishi yoki shaxsiy ma'lumotlarni suiiste'mol qilishga olib kelishi mumkin.

Kiberxujumlar nafaqat moliyaviy zarar keltirishi, balki shaxsiy, tashkilot va mamlakat darajasida jiddiy oqibatlarga olib kelishi mumkin. Shuning uchun, kiberxavfsizlikni ta'minlash va kiberhujumlarga qarshi kurashishning samarali choralarini ko‘rish juda muhim.Quyida esa kiberhujum turlari haqida ma’lumot berib o’tiladi.

kiberxujumlarning turli xil turlari va ularga qarshi kurashish usullari quyidagi tarzda bo‘lishi mumkin:

ISSN 2181-3187

1. Phishing (Soxta xat yuborish)

Tavsif: Phishing hujumlarida kiberxurujchilar foydalanuvchilarni soxta veb-saytlar yoki xabarlar orqali aldaydi. Maqsad foydalanuvchining shaxsiy ma'lumotlarini (masalan, parol, karta raqami) olishdir.

Kurashish usuli:

- Foydalanuvchilarga phishing xatlarni tanib olish bo‘yicha treninglar o‘tkazish.
- Elektron pochta xavfsizlik sozlamalarini kuchaytirish.
- Ma'lumotlarni ikki faktorlama autentifikatsiya bilan himoya qilish.
- Xavfsizlik dasturlarini va spam filtrlari o‘rnatish.

2. **DDoS (Distributed Denial of Service) Hujumlari**

Tavsif: DDoS hujumi tizimni yoki veb-saytni ishlashdan to‘xtatish uchun bir necha manbalardan bir vaqtning o‘zida katta miqdorda so‘rov yuborishdan iborat.

Kurashish usuli:

- Trafikni kuzatish va tahlil qilish.
- Tarmoqni skalalash va serverlarga yukni taqsimlash.
- DDoS hujumlarini aniqlash va himoya qilish uchun maxsus dasturlar va xizmatlardan foydalanish.
- Tarmoq xavfsizlik devorlarini (firewall) o‘rnatish.

3. **Malware (Zararli Dasturlar)**

Tavsif: Malware — kompyuterlar yoki mobil qurilmalarga zarar yetkazadigan, ma'lumotlarni o‘g‘irlaydigan yoki tizimlarni buzadigan dasturlar.

Kurashish usuli:

- Anti-virus va anti-malware dasturlarini muntazam yangilab borish.
- Tizim va ilovalarni yangilab turish.
- Shubhali manbalardan dastur yuklab olmaslik.
- Xavfsizlik devorlarini (firewall) faollashtirish.

4. **Ransomware (Ma'lumotlarni Garovga Olish)**

Tavsif: Ransomware hujumlarida zararli dasturlar qurilmalarga kirib, fayllarni shifrlaydi va foydalanuvchini shifrlangan fayllarni qaytarish uchun pul to‘lashga majbur qiladi.

ISSN 2181-3187

Kurashish usuli:

- Zaxira nusxalarini yaratish va ularni alohida saqlash.
- Ma'lumotlarni muntazam ravishda zaxiralash.
- Anti-virus va xavfsizlik dasturlarini yangilab turish.
- Xavfsiz internet tarmog‘idan foydalanish.

5. **SQL Injection (SQL Kiritish Hujumlari)**

Tavsif: Bu hujumda kiberhujumchilar veb-saytlar yoki onlayn tizimlarda ma'lumotlarni o‘g‘irlash uchun SQL so‘rovlariga zararli kod kiritadilar.

Kurashish usuli:

- Kiritish ma'lumotlarini to‘g‘ri filtrlash va tekshirish.
- Tizimdagi SQL so‘rovlarini parametrik qilib sozlash.
- Xavfsizlikni ta'minlash uchun veb dasturlarga xavfsizlik testlarini o'tkazish.
- Xavfsizlik devorlaridan foydalanish.

6. **Man-in-the-Middle (MITM) Hujumlari**

Tavsif: MITM hujumlarida hujumchi foydalanuvchi va server orasidagi aloqa kanalini o‘g‘irlaydi va ularni o‘zgartiradi, shaxsiy ma'lumotlarni o‘g‘irlaydi.

Kurashish usuli:

- SSL/TLS shifrlashdan foydalanish.
- Xavfsiz Wi-Fi tarmoqlaridan foydalanish.
- Foydalanuvchilarga HTTPS protokoli orqali faqat xavfsiz saytlarga kirishni tavsiya etish.

7. **Brute Force (Kuch bilan kirish)**

Tavsif: Brute Force hujumlarida kiberhujumchi tizimga kirish uchun turli xil parollarni avtomatik tarzda tekshiradi.

Kurashish usuli:

- Kuchli, murakkab parollarni ishlatish.
- Ikki faktorlama autentifikatsiya (2FA) qo‘llash.
- Parolni uzoq vaqtda yangilab turish.
- Hisobni bir necha marta noto‘g‘ri kiritishdan so‘ng bloklash.

8. **Cross-Site Scripting (XSS)**

ISSN 2181-3187

Tavsif: XSS hujumlarida zararli skriptlar veb-saytlarga kiritiladi, bu orqali foydalanuvchilarning brauzerlarida zararli kod ishlaydi.

Kurashish usuli:

- Kiritish ma'lumotlarini to‘g‘ri filtrlash va sanitizatsiya qilish.
- JavaScript xavfsizligini ta'minlash.
- Foydalanuvchi ma'lumotlari bilan ishlashda xavfsizlik protokollarini qo‘llash.

9. **Social Engineering (Ijtimoiy Muhandislik)**

Tavsif: Bu hujumda kiberxurujchilar odamlarni aldaydi va ulardan shaxsiy ma'lumotlarni olishga harakat qiladi.

Kurashish usuli:

- Foydalanuvchilarni ijtimoiy muhandislik usullari bilan tanishtirish.
- Ma'lumotlarni faqat ishonchli manbalar bilan almashish.
- Ichki siyosatlar va protseduralarni o‘rnatish, xodimlarni muntazam ravishda xavfsizlik bo‘yicha o‘qitish.

Har bir kiberxujum turi o‘ziga xos xavf-xatarlarni yaratadi, shuning uchun ularning oldini olish uchun xavfsizlik choralarini ko‘rish va ularni muntazam ravishda yangilab borish juda muhimdir. Bu usullar yordamida kiberxujumlarning turli turlariga qarshi samarali kurashish mumkin

Xulosa

Kiberxujumlar bugungi kunda global miqyosda katta tahdidga aylangan. Ular turli maqsadlar, jumladan, moliyaviy foyda olish, shaxsiy ma'lumotlarni o‘g‘irlash, tashkilotlar va davlat tizimlarining reputatsiyasini yo‘qotish, hamda siyosiy maqsadlar uchun amalga oshiriladi. Kiberhujumlarning oqibatlari juda jiddiy bo‘lib, ular moliyaviy zarar, ma'lumotlarning yo‘qolishi yoki buzilishi, tizimlar va xizmatlarning to‘xtashiga, shuningdek, shaxsiy hayotning buzilishiga olib kelishi mumkin.

Kiberxavfsizlik choralarini kuchaytirish, zamonaviy texnologiyalarni va xavfsizlik protokollarini joriy etish, shuningdek, foydalanuvchilarni kiberhujumlar va ularning oldini olish bo‘yicha muntazam ravishda o‘qitish kiberxavfsizlikni ta'minlashning eng samarali yo‘llaridir. Kiberhujumlarga qarshi kurashish nafaqat tashkilotlarning, balki jamiyatning xavfsizligini ta'minlashda ham muhim rol o‘ynaydi. Shunday qilib, kiberxavfsizlikni kuchaytirish va kiberhujumlarga qarshi kurashish butun dunyo bo‘yicha hamkorlikni talab qiladigan dolzarb vazifa hisoblanadi.

ISSN 2181-3187

Foydalanilgan adabiyotlar

1. **Stallings, W.** (2017). *Network Security Essentials: Applications and Standards*. Pearson

2. **Kennesaw State University.** (2019). *Cybersecurity: A Comprehensive Guide to Protecting Yourself and Your Business*. Kennesaw Press.

3. Peter Szor, "The Art of Computer Virus Research and Defense"

4. Cheswick, W. R., & Bellovin, S. M., "Firewalls and Internet Security: Repelling the Wily Hacker"

5. **Kaspersky Lab.** (2023). *Annual Threat Report: Kaspersky Security Bulletin*. https://www.kaspersky.com/about/press-releases.