

2024

JOURNAL OF INTERNATIONAL SCIENCE NETWORKS

WWW.BESTJOURNALUP.COM



AXBOROT TIZIMLARIDA KIBERXAVFSIZLIK: KIBERHUJUMLAR VA ULARDAN HIMOYALANISH USULLARI

¹ Haydarov Javlonbek Adxam o'g'li

² Norqulov Davlatbek Farhod o'g'li

³ Erkaboyev Ulug'bek Alim o'g'li

^{1,2,3} Mirzo Ulug'bek nomidagi O'zbekiston Milliy universitetining
Jizzax filiali talabalari

javlonbekhaydarov05@gmail.com

davlatnorqulov211@gmail.com

erkaboyevulugbek15@gmail.com

ANNOTATSIYA: Kiber hujum bu kompyuter tarmoqlari va tizimlarida joylashgan axborot resurslari va tizimlarini o'g'irlash, o'zgartirish, yo'q qilish, buzish yoki o'chirishga urinish bo'lib kiberhujumlar ikki toifaga bo'linishi mumkin: ichki tahdidlar yoki tashqi tahdidlar. Insayder tahdidlar o'zlari maqsad qilgan tizimlarga qonuniy kirish huquqiga ega bo'lgan shaxslarning zaifliklardan ataylab yoki beixtiyor foydalanishlari natijasida yuzaga keladi.

Kalit so'zlar: Kiber hujum, autsayder, insayder, Internet of Things, Backdoor troyan, shifrlash.

Axborot xavfsizligi - bu uzatiluvchi, yig'iluvchi va saqlanuvchi axborotning xususiyati (holati) bo'lib, uning tashqi muhit (inson va tabiat) va ichki tahdidlardan himoyalanganlik darajasini xarakterlaydi. Axborotni muhofaza qilish keng ma'noda axborot xavfsizligiga tahdidni oldini olish va ularning asoratlarini yo'q qilishga qaratilgan tashkiliy, huquqiy va texnik choralar kompleksini bildiradi. Axborotni muhofaza qilish axborotga bo'lgan salbiy ta'sir manbalarini hamda sabab va sharoitlarni aniqlash va bartaraf etish ma'nosini anglatadi. Bu manbalar axborot xavfsizligiga tahdidlarni tashkil etadi. Axborotni muhofaza qilish quyidagilarga yo'naltirilgan:

- axborot xavfsizligini ta'minlash bo'yicha tahdidlarning oldini olish;
- tizimli tahlil va nazorat orqali real va ehtimoli katta bo'lgan tahdidlarni aniqlash va ularni o'z vaqtida oldini olish choralari;
- aniq tahdidlar va jinoiy harakatlarni aniqlash maqsadida tahdidlarni topish;

Kiber hujumchilar odatda sog'liqni saqlash, hukumat, notijorat va moliya kompaniyalari kabi sohalarni nishonga olishadi. Sog'liqni saqlash sohasi ayniqsa hujumga moyil bo'ldi, chunki sog'liqni saqlash tashkilotlari ko'plab odamlarning shaxsiy ma'lumotlariga kirish huquqiga ega. Sog'liqni saqlash infratuzilmasi juda muhim bo'lganligi sababli, ransomware hujumchilari bu tashkilotlar o'z talablarini tezda to'lashlarini tushunishadi. Ijtimoiy xavfsizlik raqamlari kabi maxfiy ma'lumotlar davlat tashkilotlarining ham xakerlar qurboni bo'lishiga olib keladi. Nodavlat notijorat tashkilotlari donorlar va mablag' yig'ish harakatlarining moliyaviy ma'lumotlariga ega bo'lishi bilan ajralib turadi, bu ularni kiberhujumlar uchun ideal nishonga aylantiradi. Moliya sohasida banklar va sug'urta kompaniyalari kabi muassasalar katta miqdordagi pulga ega bo'lganligi sababli tovlamachilik va o'g'irlik uchun keng tarqalgan nishon hisoblanadi. Hujumni amalga oshiruvchi

shaxs ma'lumotlarga, funksiyalarga yoki tizimning boshqa kirish cheklangan joylariga ruxsatsiz, potensial ravishda yomon niyatda kirishga harakat qiladi. Kontekstga qarab, kiberhujumlar kiberurush yoki kiberterrorizmning bir qismi sifatida tavsiflanishi mumkin. Kiber hujum suveren davlatlar, shaxslar, guruhlar, jamiyatlar yoki tashkilotlar tomonidan qo'llab-quvvatlanishi yoki anonim manba asosida yuzaga chiqishi mumkin. Kiberhujum paytida foydalaniluvchi qurol-asboblari kiberqurollar deb ataladi. So'nggi bir necha yil ichida kiberhujumlar soni yuqori hajmda tashkil etilmoqda Kiber hujumlar moliyaviy foydadan tashqari boshqa maqsadlarga ham ega bo'lishi mumkin. Ba'zi kiberhujumlar muhim ma'lumotlarni yo'q qilishga yoki ularga kirishga qaratilgan.

Kiber hujumlarning keng tarqalgan turlari:

1. Zararli dastur

Kiber hujumchilar tizimingiz ma'lumotlariga kirish uchun josuslik dasturlari, viruslar, to'lov dasturlari va zararli dastur deb nomlanuvchi qurtlar kabi zararli dasturlardan foydalanadilar. Zararli ilova yoki havolani bosganingizda, zararli dastur o'zini o'zi o'rnatishi va qurilmangizda faollashishi mumkin.

2. Parol hujumlari

Parolga hujumlar, kimdir sizning parolingizni to'g'ri taxmin qilganidek oddiy bo'lishi mumkin yoki tajovuzkorlar siz kiritgan ma'lumotni kuzatishi va keyin parollarni aniqlashi mumkin bo'lgan keylogging kabi boshqa usullar bo'lishi mumkin. Buzg'unchi, shuningdek, yuqorida aytib o'tilgan fishing usulidan ishonchli sayt sifatida maskarad qilish va sizni aldab, hisob ma'lumotlarini oshkor qilishga urinishi mumkin.

3. Internet of Things hujumi

Ulangan IoT komponentlari orasidagi aloqa kanallari kiberhujumlarga hamda IoT qurilmalarida joylashgan ilovalar va dasturlarga sezgir bo'lishi mumkin. IoT qurilmalari internet orqali bir-biri bilan bog'langanligi va cheklangan xavfsizlik xususiyatlariga ega bo'lishi mumkinligi sababli, tajovuzkorlar nishonga olishlari mumkin bo'lgan kattaroq hujum maydoni mavjud.

4. Backdoor trojan

Backdoor trojan hujumlari zararli dasturlarni yoki ma'lumotlarni aldamchi tarzda o'rnatishi va kompyuter tizimingiz uchun "orqa eshik" deb ataladigan narsalarni ochishi mumkin bo'lgan zararli dasturlarni o'z ichiga oladi. Buzg'unchilar orqa eshikka kirish imkoniga ega bo'lganda, ular foydalanuvchiga ma'lum bo'lmasdan qurilmani o'g'irlashlari mumkin.

Kiber hujumlarning oldini olishning muhim birinchi qadami bu sizga va tashkilotingizning boshqa xodimlariga kiberhujumlar potentsialidan xabardor bo'lishdir. Havolani bosishdan oldin ehtiyot bo'lish va uning qonuniy ko'rinishini ta'minlash uchun elektron pochta manzilini tekshirish ma'lumotlaringiz va tizimlaringiz xavfsizligini ta'minlashda uzoq yo'lni bosib o'tishi mumkin.

Kiberhujumlarning oldini olish uchun bir nechta foydali usullari mavjud:

Dasturiy ta'minotni yangilash

Eng yangi dasturiy ta'minot tizimlari eskirgan versiyalarga qaraganda ancha chidamli bo'lib, ular zaif tomonlarga ega bo'lishi mumkin. Yangilanishlar dasturiy ta'minotdagi har qanday nuqson va kamchiliklarni tuzatishi mumkin, shuning uchun eng so'nggi versiyaga ega

bo'lish maqbuldir. Bundan tashqari, yamoqlarni boshqarish tizimiga sarmoya kiritish orqali dasturiy ta'minot tizimlarini yangilab turishni o'ylab ko'ring.

Xavfsizlik devorini o'rnatish

Xavfsizlik devorlari turli xil hujumlarning oldini olishda yordam beradi, masalan, orqa eshiklar va xizmat ko'rsatishni rad etish hujumlari. Ular sizning tizimingiz orqali harakatlanadigan tarmoq trafigin boshqarish orqali ishlaydi. Xavfsizlik devori kompyuter uchun potentsial zararli deb hisoblagan har qanday shubhali faoliyatni ham to'xtatadi.

Ma'lumotlarni shifrlash

Ma'lumotlarni shifrlash kiber hujumlarning oldini olishning mashhur usuli bo'lib, u ma'lumotlarga faqat shifrn ochish kalitiga ega bo'lganlar uchun ochiq bo'lishini ta'minlaydi. Shifrlangan ma'lumotlarga muvaffaqiyatli hujum qilish uchun tajovuzkorlar ko'pincha to'g'ri kalitni topmaguncha turli xil kalitlarni sinab ko'rishning qo'pol kuch usuliga tayanishi kerak, bu shifrlashni buzishni qiyinlashtiradi.

Kuchli parollardan foydalanish

Hujumlarning oldini olish va turli hisoblar va tizimlar uchun bir xil parollardan foydalanmaslik uchun kuchli parollarga ega bo'lishingiz kerak. Bir xil parolni qayta-qayta ishlatish tajovuzkorlarga barcha ma'lumotlaringizga kirish huquqini berish xavfini oshiradi. Parollaringizni muntazam yangilash va maxsus belgilar, katta va kichik harflar va raqamlarni birlashtirgan parollardan foydalanish hisoblaringizni himoya qilishga yordam beradi

Foydalanilgan adabiyotlar:

1. R.Yadava, G.Kashyapb, "Cybersecurity: Protecting Networks, Systems, and Data from Cyberattacks"
2. Anderson, R., Moore, T. (2009). Information security economics - and beyond. In T. M. Moore (Ed.), *Economics of Information Security* (Vol. 1, pp. 187-198). Springer.
3. Мустафоев Е., Холматов Ж. Brayl matn tasviri sifatini oshirish usullari //Информатика и инженерные технологии. – 2023. – Т. 1. – №. 2. – С. 23-27.
4. Холматов Д., Мустафоев Э. Zamonaviy diskret matematikaning vazifalari //Информатика и инженерные технологии. – 2023. – Т. 1. – №. 2. – С. 352-356.
5. Mustafoyev E. M., Maydonova Z. N. MOBIL ILOVA YARTISHDA FOYDALANILGAN ONLAYN APP INVERTOR PLATFORMASIDAN FOYDALANISH //Лучшие интеллектуальные исследования. – 2023. – Т. 10. – №. 6. – С. 23-28.
6. Mustafoyev E., Dustbekova M., Kamolova D. MASHINALI O 'RGANISH JARAYONIDA ENG YAXSHI QO 'SHNILAR ALGORITMINI QO 'LLASH //International Journal of scientific and Applied Research. – 2024. – Т. 1. – №. 3. – С. 84-88.
7. Mixliyev R., Mustafoyev E. MIKROSKOPDAGI TASVIRLARDA HUYAYRALARNI SANASH VA ANIQLASH ALGORITMI //International Journal of scientific and Applied Research. – 2024. – Т. 1. – №. 1. – С. 30-32.
8. Razzoq o'g'li M. R. et al. BRAYL MATN TASVIRLARIGA DASTLABKI ISHLOV BERISH USULLARI //Ta'limda raqamli texnologiyalarni tadbiq etishning zamonaviy tendensiyalari va rivojlanish omillari. – 2024. – Т. 31. – №. 2. – С. 107-110.
9. Javlon K., Erali M. STRUCTURE AND PRINCIPLE OF OPERATION OF FULLY CONNECTED NEURAL NETWORKS //International Journal of Contemporary Scientific and Technical Research. – 2023. – С. 136-141.