E CONF SERIES

Scientific Conference on Multidisciplinary Studies
Hosted online from Bursa, Turkey
Website: econfseries.com 11th January, 2025

KIBERXAVFSIZLIKNING TURLARI HAMDA JAMIYATDAGI O‘RNI

Sattorov Nazarbek Odiljonovich
Toshkent shaxar adliya boshqarmasi bosh mutaxassisi
tel: +998 97 367 1777
nazarbek.sattorov@bk.ru

Anotatsiya:
Raqamli dunyo rivojlanishi bilan kiberxavfsizlikning ahamiyati ortib bormoqda. Har bir tashkilot va shaxs o'z ma'lumotlarini himoya qilishga, tahdidlardan qochishga va kiber hujumlarni oldini olishga harakat qilmoqda. Ushbu maqolada kiberxavfsizlik tushunchasi, tahdidlar va ularni bartaraf etish choralarini ko'rib chiqamiz.

Kalit So'zlar: Axborot xavfsizligi, Kiberxavfsizlik, zararli dasturlar, phishing, DDoS hujumlari, Kuchli parollar, Ikki faktorli autentifikatsiya (2FA), Zaxiralash, Tarmoq xavfsizligi, Zero hujumlar.

Birinchi navbatda biz kiberxavfsizlik tushunchasi hamda kiberxavfsizlikni turlari haqida ma’lumotga ega bo‘lishimiz lozim.

Kiberxavfsizlik bu - qandaydir kompyuter tizimi yoki kompyuter tarmog‘i yoki foydalanuvchining raqamli ma’lumotlarini kibermuxitda ya’ni raqamli muxitda ximoyalash chora tadbirlaridir.
Kiberxavfsizlik mutaxassisi aynan shu chora tadbirlarni qo‘llashga harakat qiladi va foydalanuvchilarni yoki biron bir kompaniyalarning ichki shaxsiy ma’lumotlarini ximoyalashga harakat qiladi.
Kiberxavfsizlik mutaxassisining asosiy vazifalari bu tashkilotning qandaydir ma’lumotlari yoki tuzilmaning qandaydir ma’lumotlarini tashqi muxitdagi xujumlardan yoki kiberhujumlardan himoya qiladi. Agar tizimda yoki tashkilotning tarmog’ida kamchiliklar kuzatiladigan bo‘lsa mutaxasis aynan shuni bartaraf etishi kerak bo’ladi.
Kiberhujumlar – bu biror tashkilotning yoki kompaniyaning ichki tarmog’i yoki shaxsiy kompyuteriga qaratilgan nojo‘ya xatti-xarakatlardir.

Kiberhujum tizimga ruxsatsiz, buzib kirish orqali mo‘ljallangan nishonni o‘g‘irlashi, o‘zgartirishi yoki yo‘q qilishi mumkin. Bu turdagi hujumlar shaxsiy kompyuterga josuslik dasturlarini o‘rnatishdan tortib, biror davlat infratuzilmasini butkul yo‘q qilishga urinish kabi maqsadlarda sodir etilishi mumkin. Yuridik ekspertlar atamani jismoniy shikastlanish hodisalari bilan cheklab qo‘yishga moyil bo‘lib, odatiy ma’lumotlar buzilishiga kengroq xakerlik harakatlaridan ajratishga intilishadi.

Kiberhujum maqsadi – asosiy maqsadlardan biri bu ma’lumot o‘marish,bundan tashqari ba’zi kiberhujumchilar biror kompaniyaning ichki tarmog’ini buzish uchun shu ishni amalga oshirish mumkin.

Siyosiy maqsadga davlatlararo kiberhujumlar qilinishi mumkin. Misol uchun biror bir davlat kiberhujumchilari boshqa bir davlatning ma’lumotlar bazasini buzib uning tarmog’iga kirib maxfiy ma’lumotlarni olish uchun ishlatiladi.

Kibertahdidlar (cyber threats) — bu internet orqali amalga oshiriladigan turli hujumlar va zararli faoliyatlar bo'lib, ular tizimlarga, ma'lumotlarga yoki tashkilotlarga zarar yetkazish maqsadida amalga oshiriladi. Kibertahdidlar bir nechta shakllarda bo'lishi mumkin, va ularning har biri o'ziga xos xavf va zararlarga olib keladi.

UzCERT (Kiberxavfsizlik xizmatlariga chora ko‘rish xizmati) xizmati tomonidan 2024-yilning 5-fevralidan 11-fevraligacha mamlakat hududidagi axborot tizimlari va resurslariga nisbatan 32 156 ta kibertahdid aniqlandi. Bu haqda Kiberxavfsizlik markazi xabar bermoqda.

Ulardan eng ko‘pi hukumatga tegishli axborot tizimlariga nisbatan uyushtirilgan bo‘lib, jami ko‘rsatkichning 52,7 foizini tashkil etadi.

Shuningdek, sohalar bo‘yicha AKT (19,3 foiz),moliya (14,2 foiz), energetika (4,3 foiz) hamda ishlab chiqarish (3,9 foiz) sohalaridagi axborot tizimlariga ham kibertahdidlar sodir etilgan.

2024 yilda aynan Toshkentda o‘tkazilgan “Kibertahdidlar sammiti –Markaziy Evroosiyo CSS 2024 ” II Xalqaro kiberxavfsizlik sammiti bo‘lib o‘tdi. Bundan ko‘zlangan asosiy maqsadlardan biri jamiyatimizda va butun dunyoda kiberhujumlarni oldini olishdan iborat edi.

Quyida kibertahdidlarning asosiy turlari haqida ma'lumot berilgan:

1. Viruslar va zararli dasturlar (Malware)

Virsullar: Bu dasturlar kompyuter tizimlariga kirib, boshqa dasturlarni zararli holatga keltiradi yoki o'zini tizimga tarqatadi. Viruslar, odatda, tizimlar yoki ma'lumotlar bazasini o'zgartirish yoki yo'q qilish maqsadida ishlaydi.

Trojanlar (Trojan horses): Tizimga zarar yetkazmaydigan, lekin foydalanuvchi uchun xavfli bo'lgan dasturlar. Masalan, foydalanuvchi o'zi bilmagan holda biror zararli dastur yoki faylni o'rnatishi mumkin.

Ransomware (Talabnomali dasturlar): Ma'lumotlarni shifrlab, foydalanuvchidan ma'lumotlarni tiklash uchun pul talab qiladi.

2. Fishning (Phishing)

Phishing hujumlari foydalanuvchining shaxsiy ma'lumotlarini (masalan, parol yoki karta raqamlarini) olish uchun yolg'on yoki aldovli xabarlar yuborishni o'z ichiga oladi. Masalan, foydalanuvchiga bankdan kelgan deb ko'rsatilgan xabar orqali, uning login va parolini so'rash mumkin.

3. Denial of Service (DoS) va Distributed Denial of Service (DDoS)

DoS hujumlari: Tizimni yoki veb-saytni xizmatdan mahrum qilish maqsadida amalga oshiriladi. Bu turdagi hujumlar odatda serverga juda ko'p so'rov yuborish orqali tizimni to'liq yoki qisman ishdan chiqaradi.

DDoS hujumlari: Bu DoS hujumining yanada kengaytirilgan shaklidir, chunki bir nechta kompyuter yoki qurilmalardan hujum amalga oshiriladi. Natijada, tizimni ishdan chiqarish yanada qiyinlashadi.

Dos Attakani oldini olish uchun saytni tashqi proksi serverdan kirishi taqiqlab qo’yilish yaxshi. Hamda zarar keltiradigan IP adreslarni bloklash bu orqali tizimni ishlashini barqarorlashtiradi.

4. Man in the Middle (MitM) hujumlari

MitM hujumlari biron bir qurilma yoki foydalanuvchi bilan uzatilayotgan ma'lumotlarni o'zgartirish yoki ularga kirish uchun amalga oshiriladi. Bu turdagi hujumda, xaker foydalanuvchi va server o'rtasidagi aloqa kanaliga kirib, ma'lumotlarni ko'ra oladi yoki ularni tahrirlaydi.

5. SQL Injection

Bu hujum turi veb-saytning ma'lumotlar bazasiga kirish uchun tizimdagi xavfsizlik zaifliklaridan foydalanadi. Xaker, foydalanuvchi tomonidan kiritilgan ma'lumotlarni

manipulyatsiya qilib, serverga zarariyetli SQL buyruqlarini yuboradi, shu orqali ma'lumotlar bazasidagi maxfiy ma'lumotlarga kirishi mumkin.

6. Zero-Day Exploits

Zero-day hujumlari dasturiy ta'minotdagi noma'lum zaifliklardan foydalanadi. Bunday zaiflik ishlab chiqaruvchi tomonidan aniqlanmagan bo'lib, xakerlar bu zaifliklardan foydalanib, tizimga kirish yoki zarar yetkazish imkoniyatiga ega bo'lishadi.

7. Social Engineering

Social engineering — bu inson psixologiyasidan foydalanib, odamlarni aldanish va maxfiy ma'lumotlarni oshkor qilishga majbur qilishdir. Masalan, xakerlar telefon orqali foydalanuvchini aldab, uning parolini so'rashlari mumkin.

8. Botnetlar

Botnetlar bu kompyuter yoki qurilmalarning tarmoq orqali birlashtirilgan va xakerlar tomonidan boshqariladigan to'plamidir. Botnetlar asosan DDoS hujumlari yoki boshqa zararli faoliyatlar uchun ishlatiladi.

9. Keyloggerlar

Keyloggerlar foydalanuvchi kiritgan har bir tugmani (masalan, parollar yoki shaxsiy ma'lumotlar) yozib olish uchun mo'ljallangan dasturlardir. Keyloggerlar kompyuterga yoki mobil qurilmaga o'rnatilib, foydalanuvchining barcha yozuvlarini kuzatib borishi mumkin.

10. Advanced Persistent Threats (APT)

APT hujumlari juda murakkab va uzoq muddatli hujumlar bo'lib, ular o'z maqsadlariga erishish uchun ko'p vaqt davomida yashirin faoliyat yuritadilar. APT hujumlari ko'pincha davlatlar yoki yirik tashkilotlar tomonidan amalga oshiriladi.

Kiber hujum: ta'rifi va turlari

Kiberhujum - bu kompyuterni o'chirib qo'yish va ma'lumotlarni o'g'irlash uchun operatsion tizimni o‘g‘irlash, buzish yoki buzishning maqsadga muvofiq usulidir. Kiber hujumlarni uch turga bo‘lish mumkin:

Zararsiz (nisbatan). Bu kompyuterga zarar etkazmaydigan hujumlar. Bu ma’lumot to‘plash yoki boshqa dasturlar uchun josuslarga qarshi dasturlarning kiritilishi bo‘lishi mumkin. Xulosa shuki, odam kompyuter yuqtirganligini bilmaydi.

Zararli. Bular ham kompyuterlar, ham kompyuter tizimlarining ishlashini buzishga qaratilgan kiberhujumlardir. Aksariyat hollarda virus dasturiy ta’minoti har qanday usulda kompyuterni sabotaj qilishga, ya’ni ma’lumotlarni yo’q qilishga, shifrlashga, OSni buzishga, kompyuterlarni qayta ishga tushirishga va hokazolarni amalga oshirishga urinadi. Natijada pirovard natijada tovlamachilik va daromad va vaqtni yo’qotish hisoblanadi.

Kiber terrorizm. Kommunal xizmatlar va davlat xizmatlari qurbonga aylanadigan eng xavfli kiberhujum turi. Bunday hujumlar ayrim tuzilmalarga qaratilgan bo‘lib, ularning noto‘g‘ri ishlashi davlat infratuzilmasini zaiflashtirishi yoki yo‘q qilishi mumkin.

Hisoblarni buzish

Xakerlar har qanday shaxsning akkauntiga to'liq kirish huquqiga ega bo'lishlari mumkin, ayniqsa, "frontal hujum" dan foydalanishda, unda maxsus dasturiy ta'minot har qanday kirish / parol juftligini sinab ko'radi.

Dastur bunday ish bilan shug'ullanganligi sababli, ma'lum miqdordagi noto'g'ri kiritilgan paroldan keyin hisobni bloklashni o'rnatish kerak. Shuningdek, siz robotlardan, ya'ni reCAPTCHA tizimidan himoyadan foydalanishingiz mumkin.

Kiber mudofaa strategiyasi

Kiberhujum ehtimolini minimallashtirish uchun ba'zi muhim maslahatlar:

Antivirus va xavfsizlik devori dasturlari doimo kompyuterda ishlaydi.

Dasturiy ta'minot va operatsion tizim rasmiy yangilanishlar mavjud bo'lganda yangilanishi kerak.

Agar siz notanish kishidan xat olgan bo'lsangiz va ushbu xatda qo'shimchalar mavjud bo'lsa, ularni ochmasligingiz kerak.

Agar Internet manbai noma'lum bo'lsa, uni yuklab olish yoki undan nusxa ko'chirish tavsiya etilmaydi va siz ushbu dasturni ishga tushirmasligingiz kerak.

Har qanday Internet-resurslarga parollarni o'rnatishda ularni kamida 8 ta belgidan iborat qilish kerak va ular katta va kichik harflar, shuningdek tinish belgilari va raqamlar bo'lishi kerak.

Barcha saytlar uchun bitta, hatto murakkab paroldan foydalanishga hojat yo'q.

Ishonchli kompaniyalar va veb-saytlar firibgarlardan https kabi manzilga ega shifrlangan sahifalar mavjudligi bilan ajralib turadi.

Agar sizning kompyuteringiz yoki telefoningiz parolsiz Wi-Fi-ga ulangan bo'lsa, siz hech qanday Internet-resurslarni kiritmasligingiz kerak.

Barcha muhim fayllar va hujjatlar Internet ulanmagan joyda, boshqalar uchun xavfsiz va kirish qiyin bo'lgan joyga ko'chirilishi kerak.

Davlatlararo kibertahdidlar ko'pincha siyosiy, iqtisodiy va harbiy manfaatlarni himoya qilish yoki raqobatchilardan ustun kelish maqsadida amalga oshiriladi. Bu hujumlar ko'plab davlatlarning kiberxavfsizlikni mustahkamlash va xalqaro hamkorlikni kuchaytirishga bo'lgan ehtiyojini oshirgan. Shuningdek, davlatlar o'rtasidagi kiberurushlar an'anaviy harbiy to'qnashuvlardan farqli o'laroq, ko'pincha yashirin va noaniq shaklda amalga oshiriladi, bu esa ularga ta'sirini yanada kuchaytiradi.

Raqamlashtirishning jadal sur’atlari va zamonaviy axborot-kommunikatsiya texnologiyalarini hayotning ijtimoiy-iqtisodiy sohalariga joriy etilishi nafaqat yangi imkoniyatlarning yaratilishiga yordam beradi, balki xavfsizlikka doir yangi tahdidlarni ham o‘z ichiga oladi. Davlat organlari va boshqa tashkilotlar tomonidan kiberxavfsizlikni ta’minlash bo‘yicha ko‘rilayotgan tashkiliy-texnik chora-tadbirlarga qaramay, axborot tizimlari va resurslari faoliyatining buzilishiga, shuningdek, maxfiy ma’lumotlarning sizib chiqib ketishiga olib keladigan hodisalar soni ortib bormoqda.

Xulosa qilib aytadigan bo‘lsak:

Davlatlararo kibertahdidlar ko'pincha siyosiy, iqtisodiy va harbiy manfaatlarni himoya qilish yoki raqobatchilardan ustun kelish maqsadida amalga oshiriladi. Bu hujumlar ko‘plab davlatlarning kiberxavfsizlikni mustahkamlash va xalqaro hamkorlikni kuchaytirishga bo‘lgan ehtiyojini oshirgan. Shuningdek, davlatlar o‘rtasidagi kiberurushlar an’anaviy harbiy to‘qnashuvlardan farqli o‘laroq, ko‘pincha yashirin va noaniq shaklda amalga oshiriladi, bu esa ularga ta’sirini yanada kuchaytiradi.

Raqamlashtirishning jadal sur’atlari va zamonaviy axborot-kommunikatsiya texnologiyalarini hayotning ijtimoiy-iqtisodiy sohalariga joriy etilishi nafaqat yangi imkoniyatlarning yaratilishiga yordam beradi, balki xavfsizlikka doir yangi tahdidlarni ham o‘z ichiga oladi. Davlat organlari va boshqa tashkilotlar tomonidan

kiberxavfsizlikni ta’minlash bo‘yicha ko‘rilayotgan tashkiliy-texnik chora-tadbirlarga qaramay, axborot tizimlari va resurslari faoliyatining buzilishiga, shuningdek, maxfiy ma’lumotlarning sizib chiqib ketishiga olib keladigan hodisalar soni ortib bormoqda.

Kibertahdidlarga qarshi samarali kurashish uchun keng qamrovli va tizimli yondashuv zarur. Bu yondashuvda texnologik choralar, inson omili, xavfsizlik siyosatlari, va ta'lim alohida o'rin tutadi. Tashkilotlar va shaxslar uchun kiberxavfsizlikni kuchaytirish, tizimlarni doimiy ravishda yangilash, foydalanuvchilarni ta'limlash va xalqaro hamkorlikni rivojlantirish orqali kibertahdidlarga qarshi samarali kurashish mumkin.

Foydalanilgan adabiyotlar.

1. Hanson, F. (2012). Baked in and Wired: eDiplomacy@State. Lowy Institute for International Policy.
2. Cull, N. J. (2009). Public Diplomacy: Lessons from the Past. USC Center on Public Diplomacy.
3. Manor, I. (2019). The Digitalization of Public Diplomacy. Palgrave Macmillan.
4. Pamment, J. (2012). New Public Diplomacy in the 21st Century: A Comparative Study of Policy and Practice. Routledge.
5. Seib, P. (2012). Real-Time Diplomacy: Politics and Power in the Social Media Era. Palgrave Macmillan.
6. Melissen, J. (2005). The New Public Diplomacy: Soft Power in International Relations. Palgrave Macmillan.
7. Digital Diplomacy Review 2016. URL: http://digital.diplomacy.live/ranking-and-rating/
8. Buckley N. From Russia with likes: embassy tweets prove a hit for Moscow // Financial Times. 2017. June. URL: https://www.ft.com/content/6e9ebc52-4c68-11e7-919a-1e14ce4af89b
9. Justin Trudeau. URL: https://www.facebook.com/JustinPJTrudeau/Ingram D. Clinton says false stories on Facebook helped Trump win election // Reuters. 2017. May. URL: http://www.reuters.com/article/usa-clinton-facebook/clinton-says-false-stories-on-face- book-helped-trump-win-election-idUSL1N1IX17Z

10. Making Humans a Multiplanetary Species. URL: https://www.youtube.com/watch?v=A1Yx NYiyALg&feature=youtu.be
Official Twitter for SpaceX, the future of space travel. URL: https://twitter.com/spacex
11. Совещание послов и постоянных представителей России: стенограмма. Официальный сайт президента России. URL: http://kremlin.ru/events/president/news/15902