ISSN 2181-3187

AXBOROT INFRATUZILMASIGA TAHDID VA UNI HIMOYALASHNING ZAMONAVIY KONSEPSIYALARI

Anvarova Muqaddas Xomidjon qizi
O‘zbekiston jurnalistika va ommaviy kommunikatsiyalar universiteti
Xalqaro jurnalistika yo'nalishi 3- kurs talabasi

Annotatsiya: Kiberjinoyatlar ko'pincha iqtisodiy maqsadlarda amalga oshiriladi. Bu, masalan, o'g'irlik shaklida iqtisodiy zarar yetkazishi mumkin. Maqsadlarning boshqa turlariga siyosiy maqsadlar kiradi-asosiy davlat va siyosiy institutlarga zarar yetkazish, hokimiyat munosabatlari va hokimiyatga bo'lgan ishonch tizimini buzish. Mafkuraviy maqsadlarning uchinchi turi: Internet foydalanuvchilarini, masalan, radikal terroristik va millatchi guruhlar safiga jalb qilish maqsadida g'oyalar va mafkuralarni tarqatish. Maqsadlarning to'rtinchi turi fuqarolarga ma'naviy, psixologik zarar etkazish kabi ijtimoiy-psixologik maqsadlarni o'z ichiga oladi.

Kalit so’zlar: Kiberjinoyatlar, g'oyalar va mafkuralar, axborot xavfsizligi, IT xavfsizligi, IOT xavfsizligi, axborot xavfsizligi.

Axborot xavfsizligi (kiberxavfsizlik, ingl. - cybersecurity) - bu korxona o'z kiberaktivlarini himoya qilish uchun foydalanadigan odamlar, jarayonlar va texnologiyalarning kombinatsiyasi. Axborot xavfsizligi turli dav lat va nodavlat tashkilotlarining jarayonlari bilan belgilanadigan darajalarga optimallashtirilgan, talab qilinadigan resurslarni foydalanish qulayligi (boshqarish qobiliyati) va xavfni qoplash darajasi bilan muvozanatlashgan. Axborot xavfsizligining kichik to'plamlariga IT xavfsizligi, IOT xavfsizligi, axborot xavfsizligi va operatsion texnologiya xavfsizligi kiradi.

Axborot xavfsizligi atamasi axborot xavfsizligi, dastur xavfsizligi, tarmoq xavfsizligi, Internet xavfsizligi va muhim axborot infratuzilmasi xavfsizligi tushunchalari bilan birlashtirilgan. Standartdagi axborot xavfsizligining klassik ta'rifiga o'xshab, axborot xavfsizligi aslida xavfsizlik uchligi – maxfiylik, yaxlitlik va mavjudlik tahdidlaridan aktivlarni himoya qilish xususiyati sifatida tushuniladi, ammo ba'zi mavhum doiralarda – kiber makonni qamrab oladi[1].

Axborot texnologiyalari ijtimoiy sohalarga tobora ko'proq kirib bormoqda, bu esa turli xil kibertahdidlarning sezilarli o'sishiga olib keladi va milliardlab odamlar ongida jiddiy o'zgarishlarga olib keladi. Kasperskiy laboratoriyasi tomonidan olib borilgan tadqiqotlar natijasida 10 ta kompaniyadan 9 tasi muntazam ravishda tashqi kiber tahdidlarga duch kelishi aniqlandi. 2016-yilda so'rovda ishtirok etgan vakillarining

[1] Quirk, S. Concordia Password Security Policy. Onttrek Sep. 26, 2015 uit http://kb.cu-portland.edu/Password+Security available under a Creative Commons Attribution 3.0 License.

ISSN 2181-3187

91% xorijiy va 96% Rossiya kompaniyalari axborot xavfsizligi tahdidlariga duch keldi. Moliyaviy tashkilotlarga qaratilgan ko'plab kiberhujumlar amalga oshirildi va katta moliyaviy yo'qotishlar va ishlamay qolishlarga olib keldi. Banklar, tijorat tashkilotlari va hattoki davlatlarning ishchanlik obro‘siga katta zarar yetkazildi.

Eng ko'p zarar ko'rganlar orasida Ukraina energiya tarmoqlari, Bangladesh Markaziy banki, Butunjahon antidoping agentligi (WADA) bor. Ko'pgina tashkilotlar kiberjinoyatchilardan jabr ko'rdi: masalan, xorijiy kompaniyalarga qilingan virus hujumlarining uchdan bir qismi ma'lumotlarning yo'qolishiga olib keldi, firmalarning 10 foizi uchun esa bu biznes uchun muhim ma'lumotlar edi. Xakerlar jismoniy shaxslarni ham chetlab o’tmagan: LinkedIn va Yahoo’dan yuz millionlab foydalanuvchi akkauntlari va parollari o‘g‘irlangan. Kiberhujumlar dunyodagi siyosiy vaziyatga jiddiy ta'sir ko'rsatdi: u AQSh Demokratik partiyasidan maktublarning sizib chiqishi, Mossack Fonseca ofshor hisoblarining oshkor etilishi va Fancy Bear guruhining faoliyati kiberxujum natijasida o'zgardi.

Kiberjinoyatlar ko'pincha iqtisodiy maqsadlarda amalga oshiriladi. Bu, masalan, o'g'irlik shaklida iqtisodiy zarar yetkazishi mumkin. Maqsadlarning boshqa turlariga siyosiy maqsadlar kiradi-asosiy davlat va siyosiy institutlarga zarar yetkazish, hokimiyat munosabatlari va hokimiyatga bo'lgan ishonch tizimini buzish. Mafkuraviy maqsadlarning uchinchi turi: Internet foydalanuvchilarini, masalan, radikal terroristik va millatchi guruhlar safiga jalb qilish maqsadida g'oyalar va mafkuralarni tarqatish. Maqsadlarning to'rtinchi turi fuqarolarga ma'naviy, psixologik zarar etkazish kabi ijtimoiy-psixologik maqsadlarni o'z ichiga oladi.

Yangi texnologiyalarning paydo bo'lishi, Intranet provayderlarining yaxshilanishi bilan har bir inson virtual muhitga tobora ko'proq sho'ng'iydi, bu quyidagilarni anglatadi: yangi imkoniyatlar qanchalik ko'p bo'lsa, har birimiz yangi muammolarga, xususan, Intranet firibgarligiga duch kelishimiz ehtimoli shunchalik yuqori bo'ladi[2].

Xorijiy va mahalliy olimlar ushbu turdagi jinoyatlarning nomi to'g'risida kelishmovchiliklarga duch kelishmoqda. Ilm-fan va qonunchilikda turli mamlakatlarda "kompyuter ma'lumotlari aylanmasi xavfsizligi sohasidagi jinoyatlar", "kompyuter jinoyatlari", "axborot jinoyatlari", "yuqori texnologiyalar sohasidagi jinoyatlar", "kiber jinoyatlar" va boshqalar kabi nomlar mavjud.

Ushbu sohada ishlatiladigan atamalarni aniqlashga qaratilgan birinchi urinishlardan biri bu a'zo davlatlar o'rtasidagi hamkorlik to'g'risidagi bitim edi. Mustaqil davlatlar Hamdo'stligi 2001-yilda Minskda imzolangan kompyuter ma'lumotlari jinoyatlariga qarshi kurashda shartnomasi shulardan biri hisoblanadi. Ushbu hujjatning 1 - moddasiga binoan "kompyuter ma'lumotlari sohasidagi

[2] Networking in Windows 7. (s.j.). Onttrek Oct. 24, 2015 uit http://www.utilizewindows.com/: http://www.utilizewindows.com/7/networking/452-working-with-windows-firewall-inwindows-7 available under under a Creative Commons Attribution-NonCommercialShareAlike 4.0 International License

ISSN 2181-3187

jinoyatlar" jinoiy jinoyat bo'lib, unga tajovuz mavzusi kompyuter ma'lumotlari hisoblanadi.

Kiberjinoyatchilik deganda virtual makonda kompyuter tizimlari yordamida yoki kompyuter tarmoqlari va virtual makonga kirishning boshqa vositalaridan foydalangan holda, kompyuter tarmoqlari doirasida, shuningdek kompyuter tizimlari, kompyuter tarmoqlari va kompyuter ma'lumotlariga qarshi sodir etilgan jinoyatlar majmui tushuniladi.

Tahdid manbai xavfsizlik tahdidining potentsial antropogen, texnogen yoki tabiiy tashuvchilari hisoblanadi. Tahdid (harakat) - muhofaza qilish ob'ektiga (axborot resurslariga) qarshi qaratilgan har qanday harakat (harakat yoki harakatsizlik) sodir etilishining mumkin bo'lgan (potentsial yoki real) xavfi bo'lib, uning egasiga, egasiga zarar etkazishi va axborotni buzish va yo'qotishdir. Faktor (zaiflik) - bu axborotlashtirish ob'ektiga xos bo'lgan, ma'lum bir ob'ektda axborot xavfsizligining buzilishiga olib keladigan va axborotlashtirish ob'ektining ishlashidagi kamchiliklar, avtomatlashtirilgan tizim arxitekturasining xususiyatlari, birja protokollari dasturiy va apparat platformasi tomonidan ishlatiladigan interfeyslarni buzishni qamrab oladi[3].

Kompyuter viruslari axborot xavfsizligiga asosiy tahdidlardan biri hisoblanadi. Ushbu hodisaning tarqalish ko'lami va natijada axborot tizimlariga katta zarar yetkazilishi bilan bog'liq.

Zamonaviy kompyuter virusi oddiy foydalanuvchi uchun deyarli ko'rinmaydigan va doimiy ravishda takomillashtirilib, foydalanuvchilarning kompyuterlariga kirib borishning yangi va yanada murakkab usullarini topadigan "dushman" dir. Kompyuter viruslari bilan kurashish zarurati ularning axborot xavfsizligining barcha komponentlarini buzish ehtimoli bilan bog'liq.

Hozirgi vaqtda barcha kiber tahdidlar odatda tashqi va ichki bo'linadi. Tashqi tahdidlarning sabablari va manbalari kompaniya kompyuterlaridan tashqarida, odatda global tarmoqda. Ichki tahdidlar faqat kompaniya xodimlariga, dasturiy ta'minot va texnik vositalariga bog'liq.

Tashqi tahdidlarga quyidagilar kiradi:

- viruslar;
- spam;
- fishing;
- masofaviy xakerlik;
- DoS/DDoS hujumlari;
- mobil qurilmalarni o'g'irlash.

Kibertahdidlarning asosiy xavfi ularning o'zgarishi tezligidir. Viruslar kompyuter tizimlariga yashirincha kirib boradi va samarali himoyasiz ular bilan kurashish mumkin

[3] Nandanwar, R. Case Study of Recent Examples of Cyber Crime and E-Commerce Fraud related Investigations involving IPR and Copyright Act. 2013.p.97.

ISSN 2181-3187

emas. Viruslar kompyuterga kirib borishi uchun elektron pochtada ilovani ochish kifoya (xat noma'lum adresat tomonidan yuborilgan bo'lishi shart emas, taniqli hamroh ham virus yuborishi mumkin. agar uning kompyuteri ilgari yuqtirilgan bo'lsa). Ba'zi viruslar uchun kompyuterning virusli kompyuter ham ulangan mahalliy tarmoqqa ulangan bo'lishi kifoya. Ko'p sonli viruslarni tarqatish uchun olinadigan xotira qurilmalari (flesh-disklar, mobil qattiq disklar va optik vositalar) ishlatiladi.

Litsenziyasiz (pirat) dasturiy ta'minotdan foydalanish foydalanuvchi hisobi ma'lumotlarining yo'qolishiga, noqonuniy dastur o'rnatilgan qurilmaning bloklanishiga olib kelishi mumkin. Noma'lum zararli dasturlar soni o'sishda davom etmoqda: tadqiqotchilar tashkilotlarga hujum qiladigan noma'lum dasturlar soni 9 barobarga oshganini hujjatlashtirdi. Mutaxassislar har oy zararli dasturlarning deyarli 12 million yangi variantini topadilar. Hozirda virus yaratuvchilari ulardan asosan moliyaviy manfaatlar uchun foydalanmoqda. 2016-yilda ransomware tomonidan o'z qurbonlaridan talab qilingan o'rtacha to'lov 266 foizga oshdi.

WannaCry ransomware - hujumi 150 mamlakatda 230 000 dan ortiq qurilmalarni zararlagan. Troyan virusi bank hisobi ma'lumotlarini to'sib qo'ysa, bu yanada xavflidir. Viruslar kompyuterlar va dasturlarning ishlashini buzishi, fayllarni yo'q qilishi, trafikdan, aloqa kanallaridan o'z maqsadlari uchun foydalanishi, spam yuborishi mumkin. Eng xavfli virus bu kiberqurol bo‘lib, u ayrim hollarda sanoat infratuzilmasini yo‘q qilishga qaratilgan. Duqu, Stuxnet, Gauss, Flame viruslarining paydo bo'lishi bir million dollardan oshadi. Spam nafaqat foydalanuvchilarni bezovta qiladi, balki aloqa kanallarini yopib qo'yadi, trafikni sarflaydi, ishdan chalg'itadi, odamlarni reklamalar orasidan muhim yozishmalarni izlashga majbur qiladi. Oxir oqibat, bularning barchasi moliyaviy yo'qotishlarga olib keladi. Bundan tashqari, spam ham troyan va viruslarni kiritish uchun eng keng tarqalgan kanallardan biridir. Fishing, spamdan farqli o'laroq, foydalanuvchilarning tor guruhlariga qaratilgan bo'lib, ijtimoiy kontekstli xabarlarni o'z ichiga oladi, potentsial qurbonni bajariladigan faylni ochishga yoki zararli kodni o'z ichiga olgan saytga o'tishga chaqiradi[4].

Masofaviy kompyuterni buzish ham katta xavf tug'diradi, buning natijasida tajovuzkorlar fayl serverlarida va kompyuterlarda saqlangan hujjatlarni o'qish va tahrirlash, ularni o'z xohishiga ko'ra yo'q qilish, raqobatchilarning barcha harakatlarini kuzatib boradigan va ma'lum ma'lumotlarni to'playdigan o'z dasturlarini joriy qilishlari mumkin. noutbuk mikrofonlari va standart veb-kameralar orqali sezilmaydigan audio va video kuzatuvga (Search Engine Optimization) infektsiyasi zararli kodni o'z ichiga olgan saytlarni so'rovni kiritganingizda qidiruv tizimi reytingidagi yuqori o'rinlar bilan almashtirilishiga olib keladi. Siz o'zingizni bunday tahdidlardan shlyuz antivirusining

[4] Kessler, G. C. The Role of Computer Forensics in Law Enforcement. Onttrek Dec. 20, 2015 uit http://www.garykessler.net/library/role_of_computer_forensics.html

ISSN 2181-3187

so'nggi versiyalari va hujumni oldini olish tizimlaridan himoya qilishingiz mumkin. Deyarli barcha zararli dasturlar mashhur ijtimoiy tarmoqlar orqali tarqatilishi mumkin.

Internetdagi xavfning yana bir sohasi shaxsiy xavfsizlikka tahdiddir. Bu mobil qurilmalarning paydo bo'lishi bilan bog'liq. Foydalanuvchi tranzaktsiyalar tashkilotchilariga uning zarari uchun ishlatilishi mumkin bo'lgan katta miqdordagi shaxsiy ma'lumotlarni berishga majbur bo'ladi. Android troyanlari Android mahsulotlari foydalanuvchilari uchun alohida e'tiborga loyiqdir, ularning tarqalishi Android-ning asosiy muammolari bilan bog'liq:

• zaif xavfsizlik tizimiga ega bo'lgan operatsion tizimlarning eski versiyalaridan keng foydalanish;

• turli xil mobil qurilmalar, ularning ba'zilari uchun yangilanishlar oddiygina mavjud emas;

• soxta va virusli ilovalarni yuklab olishingiz mumkin bo'lgan juda ko'p uchinchi tomon bozorlari.

Apple mahsulotlari foydalanuvchilari ham o'zlarini butunlay xavfsiz his qila olmaydi. Yangi texnologiyalar, ayniqsa, ularning professional kibermudofaasi bo'lmagan taqdirda ham xavf tug'diradi. 2016-yilda mamlakatimiz axborot resurslariga 50 milliondan ortiq kiberhujum amalga oshirildi, bu 2015-yilga nisbatan uch barobar ko‘pdir. O‘zining muhim axborot infratuzilmasini ishonchli himoya qilish uchun oqibatlarini aniqlash, oldini olish va bartaraf etish davlat tizimini yaratdi[5].

Kompyuter viruslari axborot yo'qotilishining eng keng tarqalgan sabablaridan biri bo'lib kelgan va shunday bo'lib qoladi. Virusli epidemiyalar tashkilot va korxonalar ishiga to‘sqinlik qilishi mumkin.

Raqobatchi antivirus firmalarining ulkan sa'y-harakatlariga qaramay, kompyuter viruslari tufayli yo'qotishlar kamaymaydi va har yili yuzlab million dollar astronomik qiymatlarga yetadi.

So'nggi paytlarda virusli epidemiyalar shunchalik ommaviy va tahdidli bo'lib qoldiki, ular haqidagi xabarlar dunyo yangiliklarida birinchi o'ringa chiqdi. Ammo shuni yodda tutingki, virusga qarshi dasturiy ta'minot va texnik vositalar viruslardan himoyalanishning to'liq kafolatini ta'minlamaydi va ko'pchilik foydalanuvchilarda viruslardan "himoya qilish" uchun asosiy ko'nikmalar ham yo'q.

"Kompyuter virusi" atamasi 80-yillarning o'rtalarida AQShda o'tkazilgan axborot xavfsizligi konferentsiyalaridan birida paydo bo'lgan. O'shandan beri ko'p vaqt o'tdi, viruslar muammosining jiddiyligi ko'p marta oshdi, ammo hali ham kompyuter virusining qat'iy ta'rifi yo'q.

[5] Kerberos Authentication. (s.j.). Onttrek Sep. 26, 2015 uit Interactiva: http://computers.interactiva.org/Security/Authentication/Kerberos/ available under a Creative Commons Attribution-ShareAlike 3.0 Unported License

ISSN 2181-3187

Kompyuter viruslarining asosiy xususiyati ularning operatsion tizimning turli ob'ektlariga o'z-o'zidan kirib borish imkoniyatidir - bu virus bo'lmagan ko'plab dasturlarga xosdir, ammo bu o'ziga xos xususiyat kompyuter virusining majburiy (zarur) xususiyatidir. Zamonaviy kompyuter virusini to'liqroq tavsiflash uchun o'z-o'zidan dublikatlarni yaratish (asl nusxa bilan bir xil bo'lishi shart emas) va ularni kompyuter tarmoqlari yoki fayllariga, kompyuter tizimining hududlariga va boshqa bajariladigan ob'ektlarga kiritish qobiliyatini qo'shish kerak.

Dasturiy ta'minot virusi - bu avtomatlashtirilgan tizimlarda saqlanadigan dasturiy ta'minotni va ma'lumotlarni o'zgartirish yoki yo'q qilish uchun avtomatlashtirilgan tizimlarda yoki telekommunikatsiya tarmoqlarida ruxsatsiz tarqatish va o'z-o'zini takrorlash xususiyatiga ega bo'lgan bajariladigan yoki talqin qilinadigan dastur kodi.

Shundan kelib chiqqan holda shuni tushunish kerakki, viruslardan yetarlicha dasturiy va apparat himoyasi mavjud emas va viruslardan ishonchli himoyani ushbu vositalardan kompleks foydalanish va eng muhimi, elementar “kompyuter gigienasiga” rioya qilish orqali ta’minlash mumkin.

Parolning murakkabligi (yoki kuchi, kuchi) parolni taxmin qilish yoki uni qandaydir usul bilan, masalan, katta kuch bilan taxmin qilish uchun zarur bo'lgan vaqt o'lchovidir. Tajovuzkorga parolni taxmin qilish uchun o'rtacha qancha urinish (vaqt) ketishini taxmin qilish. Terminning yana bir ta'rifi - parol uzunligi, uning murakkabligi va oldindan aytib bo'lmaydigan funksiyasi hisoblanadi.

Zaif parol - bu osongina taxmin qilinadigan yoki qo'pol tarzda buzish mumkin bo'lgan parol. Kuchli parol - bu taxmin qilish qiyin bo'lgan va qiyin qidiruv orqali tanlash uchun uzoq vaqt talab qilinadigan parol.

Murakkab parollardan foydalanish tajovuzkorning parolni taxmin qilish vaqtini oshiradi, ammo boshqa xavfsizlik choralarini qo'llash zaruratini bartaraf etmaydi. Muayyan kuchdagi parolning samaradorligi autentifikatsiya tizimlarining dasturiy ta'minotini loyihalash va amalga oshirishga, xususan, autentifikatsiya tizimi tajovuzkor parolni taxmin qilishga urinayotganda unga qanchalik tez javob berishiga va parol ma'lumotlari qanchalik xavfsiz saqlanishiga bog'liq. Xatarlar, shuningdek, parolning murakkabligi bilan bog'liq bo'lmagan kompyuter xavfsizligini buzishning ba'zi usullari bilan ifodalanadi. Bular fishing, keylogging, telefon tinglash, ijtimoiy muhandislik, axlat qutisida foydali ma'lumotlarni qidirish, yon kanal hujumlari, dasturiy ta'minotning zaifliklari, backdoorlar, ekspluatatsiyalar kabi usullardir.

Parolning murakkabligini aniqlaydigan ikkita omil mavjud:

1) tajovuzkor taxmin qilingan parolning haqiqiyligini tekshirish qulayligi;

2) tajovuzkor to'g'ri parolni topish uchun qilishi kerak bo'lgan o'rtacha urinishlar soni.

ISSN 2181-3187

Birinchi omil parolning qanday saqlanishi va u nima uchun ishlatilishi bilan belgilanadi. Ikkinchi omil parol uzunligi, foydalanilgan belgilar to'plami va parol qanday yaratilganligi bilan belgilanadi.

Parollar avtomatik ravishda (tasodifiy sonlar generatorlari yordamida) yoki shaxs tomonidan yaratiladi. Shafqatsiz kuchlar hujumi uchun parolning kuchini aniq hisoblash mumkin. Ko'pgina hollarda parollar odamlar tomonidan yaratiladi, masalan, kompyuter tizimlari yoki veb-saytlar uchun hisob yaratishda. Odamlar maslahatlar yoki qoidalar to'plami asosida parollar yaratadilar, lekin tajovuzkorning qo'lida o'ynaydigan naqshlarga amal qilishadi. Tez-tez tanlangan parollar ro'yxati parolni taxmin qilish dasturlarida foydalanish uchun keng tarqalgan[6].

Ko'p foydalanuvchili kompyuter tizimlarida parollarni bir necha o'n yilliklar davomida tahlil qilish shuni ko'rsatdiki, parollarning 40% dan ortig'ini faqat kompyuter dasturlari yordamida osongina taxmin qilish mumkin va hujum paytida ma'lum bir foydalanuvchi haqidagi ma'lumotlar hisobga olinsa, undan ham ko'proq narsani taxmin qilish mumkin.

Avtomatik parol yaratish, agar to'g'ri bajarilgan bo'lsa, parol va uning foydalanuvchisi o'rtasidagi har qanday aloqani oldini olishga yordam beradi. Masalan, foydalanuvchining uy hayvonlari nomi bunday tizim tomonidan yaratilishi dargumon. Yetarlicha katta imkoniyatlardan tanlangan parol uchun qidiruv deyarli imkonsiz bo'lib qolishi mumkin. Biroq, haqiqatan ham tasodifiy parollarni yaratish qiyin bo'lishi mumkin va odatda foydalanuvchi uchun eslab qolish qiyin.

Yaxshi parolni tanlash bo'yicha tavsiyalar parolni xakerlarning turli hiylalariga chidamliroq qilish uchun mo'ljallangan.

Tavsiya etilgan minimal parol uzunligi 12 dan 14 tagacha belgidir. Parol uzunligini atigi 2 belgiga oshirish alifboni 18 belgiga oshirishdan 500 baravar ko'proq topish imkoniyatlarini qiyinlashtiradi. Lekin shunga qaramasdan iloji bo'lsa, tasodifiy parollarni yaratish tavsiya etiladi.

Lug'at so'zlarini ("parol"), takroriy harflar to'plamini ("parol"), alifbo yoki raqamli ketma-ketlikni ("aaa", "123"), taxalluslar, ismlar (o'z ismi, qarindoshlarning ismlari uy hayvonlarining taxalluslari, romantik murojaatlar (hozirgi yoki o'tmish), biografik ma'lumotlar) o'z ichiga olgan parollardan foydalanishdan qochish tavsiya etiladi.

Agar tizim ruxsat bergan bo'lsa, parolga raqamlar va boshqa belgilarni kiritish tavsiya etiladi. Iloji bo'lsa, katta va kichik harflardan foydalanish tavsiya etiladi. Biroq, har safar to'g'ri joylarda Shift tugmachasini bosgandan ko'ra parolga so'z qo'shgan ma'qul. Turli saytlar yoki maqsadlar uchun bir xil paroldan foydalanmaslik tavsiya

[6] Hacker (computer security). (Nov.). Onttrek Dec. 20, 2015 uit 2015: http://en.wikipedia.org/wiki/Hacker_(computer_security) available under the Creative Commons Attribution-ShareAlike License.

ISSN 2181-3187

etiladi. Ba'zi tavsiyalar parolni hech qanday joyga yozmaslikni maslahat beradi, boshqalari foydalanuvchi kirish huquqiga ega bo'lishi kerak bo'lgan ko'p sonli parol bilan himoyalangan tizimlar mavjudligini ta'kidlab, parollarni yozish g'oyasini ma'qullaydi, agar, albatta, parollar ro'yxati xavfsiz joyda bo'ladi[7].

Ba'zi o'xshash parollar boshqalarga qaraganda zaifroq. Masalan, lug'at so'zidan iborat parol bilan chalkash so'zdan iborat parol o'rtasidagi farq (ya'ni, harflar o'xshash uslubdagi raqamlar bilan almashtirilgan so'z, masalan: "o" dan "0", "h" dan "4" gacha) parolni sindirish uchun qo'shimcha soniyalar ketishi mumkin - bu parolga biroz murakkablik qo'shadi. Quyidagi misollar zaif parollarni yaratishning turli usullarini ko'rsatadi. Usullar oddiy naqshlardan foydalanadi, bu esa natijada olingan parollarning past entropiyasini tushuntiradi.

Standart parollar: "parol", "standart", "admin", "mehmon" va boshqalar. Standart parollar ro'yxati Internetda keng tarqalgan.

- Lug'at so'zlari: "xameleon", "RedSox", "sandbags", "bunnyhop!", "IntenseCrabtree" va boshqalar, shu jumladan inglizcha bo'lmagan lug'atlardan olingan so'zlar.

- Raqamlar qo'shilgan so'zlar: "password1", "deer2000", "Shavkat1234" va boshqalar. Bunday parollarni tanlash juda tez amalga oshiriladi.

- Harflari almashtirilgan so'zlar: "p@ssw0rd", "l33th4x0r", "g0ldf1sh" va boshqalar. Bunday parollar oz vaqt bilan avtomatik tarzda tekshirilishi mumkin.

- Umumiy klaviatura ketma-ketliklari: "qwerty", "12345", "asdfgh", "fred" va boshqalar.

- keng tarqalgan raqamlar to'plami: "911", "314159...", "271828...", "112358..." va boshqalar.

Shaxsiy ma'lumotlar: "ivpetrov123", "1/1/1970", telefon raqami, foydalanuvchi nomi, TIN, manzil va boshqalar.

Ba'zi hujum parollarning murakkabligiga qarab, parolning zaif bo'lishi uchun boshqa ko'plab imkoniyatlar mavjud; asosiy tamoyil - parol yuqori entropiyaga ega bo'lishi va ba'zi aqlli belgi yoki shaxsiy ma'lumotlar bilan aniqlanmasligi kerak. Onlayn xizmatlar ko'pincha xaker parolni topish uchun foydalanishi mumkin bo'lgan parolni tiklash variantini taqdim etadi. Savolga taxmin qilish qiyin bo'lgan javobni tanlash parolingizni himoya qilishga yordam beradi.

Odatda odamlarga hech qachon parollarini hech qayerga yozmaslik va turli hisoblar uchun bir xil paroldan foydalanmaslik tavsiya etiladi. Shunga qaramay, oddiy foydalanuvchilar o'nlab hisoblarga ega bo'lishi mumkin va barcha hisoblar uchun bir xil paroldan foydalanishlari mumkin. Ko'pgina parollarni eslab qolmaslik uchun siz

[7] Glass, E. The NTLM Authentication Protocol and Security Support Provider. Onttrek Sep. 26, 2015 uit ourceforge: http://davenport.sourceforge.net/ntlm.html available under permission by the owner to use, copy, modify, and distribute this document for any purpose and without any fee.

ISSN 2181-3187

maxsus dasturlardan foydalanishingiz mumkin - parollarni shifrlangan shaklda saqlash imkonini beruvchi parol menejeridan foydalaniladi. Shuningdek, siz parolni qo'lda shifrlashingiz va shifrlash usulini va kalitni eslab qolgan holda qog'ozga yozishingiz mumkin. Bundan tashqari, oddiy hisoblar uchun parollarni biroz o'zgartirishingiz va yuqori qiymatli hisoblar uchun murakkab va turli xil parollarni tanlashingiz mumkin, masalan, Internet-banking.

Red Teaming formatidagi kiber ta'lim yetuk axborot xavfsizligi darajasiga ega kompaniyalar uchun eng samarali hisoblanadi. Ular ta'sir qilish vaqti bilan cheklanmaydi va tarmoq tugunlariga kirish yoki mavjud bo'lgan har qanday usul bilan sezgir ma'lumotlarga ega bo'lishdan qat'i nazar, belgilangan maqsadlarga erishishga qaratilgan.

Red Teaming-ning asosiy ssenariylari, shuningdek, har bir mijozga xos bo'lgan maqsadlarga bog'liq. Eng ko'p ishlatiladigan skriptlarga quyidagilar kiradi:

• Active Directory-ni yozib olish;

• yuqori boshqaruv qurilmalariga kirish;

• mijozning yoki intellektual mulkning sezgir ma'lumotlarini "o'g'irlash" ni taqlid qilish. Shunga o'xshash kiberhujum vositalari Red Teaming va penetratsion testlarda qo'llanilishiga qaramay, ikkala tadqiqotning maqsadlari va natijalari juda farq qiladi. Red Teaming jarayoni butun tashkilotga haqiqiy va maqsadli hujumlarni taqlid qiladi. Ushbu yondashuvning afzalligi maqsadlarga erishish uchun axborot tizimlarini doimiy ravishda o'rganishdir. Bunday chuqur tekshiruv infratuzilmaning qanchalik himoyalanganligi, xodimlarning xabardorligi va tashkilotning ichki jarayonlari haqiqiy hujumga uchraganda samarali ekanligi to'g'risida to'liq tushuncha beradi.

Foydalanilgan adabiyotlar:

1. Daniel Arp, Michael Spreitzenbarth, Malte Hubner, Hugo Gascon, and Konrad Rieck. 2014. DREBIN: Effective and Explainable Detection of Android Malware in Your Pocket. In Proceedings of the 20th Network and Distributed System Security Symposium (NDSS).
2. Fischer A., Igel C. Training restricted Boltzmann machines: An introduction // Pattern Recognition. 2014. Vol. 47. No. 1. P. 25-39
3. Goodfellow I., Bengio Y., Courville A. Deep learning // MIT press. 2016. 800 p.
4. Herath, T., Khanna, P., & Ahmed, M. (2022). Cybersecurity Practices for Social Media Users: A Systematic Literature Review. Journal Of Cybersecurity and Privacy, 2(1), 1-18
5. Johnson. R. (2016). S. 2517 (114th): Combat Terrorism Use of Social Media Act of 2016. Retrieved 22 November 2017,
6. Khan, N., Ikram, N., Murtaza, H., & Asadi, M. (2021). Social media users and cybersecurity awareness: predicting self-disclosure using a hybrid artificial intelligence approach