PASSWORD SECURITY IN INFORMATION TECHNOLOGY

Scientific researcher Mullajonov Baxodirjon Arabboyevich

Uzbekistan University of journalism and Mass Communications.

Annotation

This scientific article explores aspects that need to be considered in the proper organization of security in Information Technology. Also in the process of choosing a password are given the necessary recommendations for applying various methods, choosing the optimal options from within them.

Key words: Axborot xavfsizligi, parol, axborot texnologiyalari, kompyuter viruslari, kiberxavfsizlik.

Kompyuter texnologiyalari kun sayin rivojlanib borayotgan bugungi kunda xavfsizlik tushunchasiga extiyoj kuchayib bormoqda. Kompyuter tarmoqlari rivojlanib borgani sari, tarmoqlardan bo‘ladigan tahdidlar soni ko‘payib bormoqda. Shundan kelib chiqib, biz o‘zimizni xatar va texnologiyalar bilan birga keladigan tahdidlardan himoya qilishimiz kerak.

Internet tajovuzkorga sayyoramizning istalgan joyidan turib ishlashga imkoniyat yaratib beradi. Xavfsizlik bo‘yicha past amaliyot va bilim tufayli yuzaga keladigan xatarlar:

- Shaxsni o‘g‘irlash;
- Pul o‘g‘irlanishi;
- Huquqiy imtiyozlarga ruxsat etilmagan shaxslarni ega chiqishi;
- Agar qoidalarga rioya qilinmasa, sanksiyalar va jinoiy javobgarlik.

Axborot xavfsizligining eng muhim sohalaridan biri: parollar xavfsizligi va ishonchliligidir. Boston universiteti olimlari bergan ma’lumotlariga ko‘ra parollarni buzish uchun o‘ta qiyin va eslab qolishga juda oson shakIlda tanlash imkoni bor.

Parolingizni mustahkam bo‘lishi va parol buzuvchi zararkunanda dasturlar orqali osongina buzilmasligi uchun parollarni tanlashda quyidagilarga e’tibor berish kerak:

- Parolingizda alfabit harflari bilan birgalikda raqamlar xam ishtirok etsin;
- Imkon boricha maxsus belgilar @ # $ % ^ & * dan foylanishga harakat qiling, ammo bo‘shliqdan foydalanmang. Chunki, ba’zi tizimlar parollardagi bo‘shliqlarni hisobga olmaydi;
- Harf, belgi, raqamlardan so‘zlar yasashga harakat qiling. Masalan: “azamat” so‘zini a3@/\\at shaklida yozish mumkin;
- So‘zlarni imloviy xatolar bilan, talaffuziga ko‘ra yozishga harakat qiling. Masalan: “falokat” so‘zini palakat ko‘rinishida yozish mumkin;
- Bir – biriga ma’no jihatidan mos kelmaydigan so‘zlardan foydalaning. Masalan: sovuqolam;
- Harflar yoki raqamlarni belgilar bilan, raqamlarni harflar bilan, harflarni esa raqamlar bilan almashtirib yozing. Masalan: b@)(0№a (“baxona” yozilgan)

Parol tanlash bosqichida ko‘pchilik uchun qiyin bosqich bo‘lishi mumkin. Shunday parol tanlash kerakki, u boshqalar uchun qiyin bo‘lishi bilan odamni o‘zini esida qolishga oson bo‘lishi kerak.

Parol xavfsizligida eng muhim narsalardan yana biri – bitta parolni barcha tizimlar uchun bir xil ko‘rinishda ishlatmaslik kerak. Juda ko‘pchilik bu xatoga yo‘l qo‘yadi. Bu xatoga yo‘l qo‘yilganda, sizni bir tarmoqdagi parolingizni buzishlari orqali boshqa tizimlardagi xavfsizligingiz xam 0 ga teng bo‘ladi.

Parol buzuvchi juda ko‘p zararkunanda dasturlar ishlab chiqilgan va bular keng foydalanishga chiqib ketkan. Shu bilan birgalikda bunday dasturlarni istalgan dasturchi yaratishi xam mumkin. Bu dasturlar parolni qayta qayta terish orqali sizni parolingizni topishga urinib ko‘radi.

Bu dasturlar quyidagi holatlarda nechta urinishda topishi quyida aks etgan:

- Parol lotin alfabitida inglizcha so‘zdan iborat bo‘lsa – tahminan 600 000 ta urinish;
- Parol faqat raqamdan iborat bo‘lsa – 100 000 000 urinish;
- Parol faqat kichik harflarda bo‘lsa – 208 827 064 576 urinish;
- Parol katta va kichik harflardan iborat bo‘lsa – 53 459 728 531 456 urinish;
- Parol raqam, harf va belgilardan iborat bo‘lsa – 1 853 020 188 851 840 urnish.

Parollarda xavfsizlikni yaxshi o‘rnatish uchun parollarning uzunligi ham ahamiyatga ega. Masalan:

- 8 belgi, harf, raqamli parol 645 trillion kombinatsiyada;
- 9 belgi, harf, raqamli parol 45 kvadrilion kombinatsiyada;
- 10 belgi, harf, raqamli parol 3 kvintrillion kombinatsiyada topishi mumkin.

Parollardan foydalanishda imkon qadar shaklda tanlashga harakat qilish kerak. Ma’lumotlarni xavfsizligiga jiddiy qarash kerak va sodda parollardan foydalanmaslik kerak.

Butun dunyoda parol murakkab bo‘lsa xavfsizligi oshadi deb kelinsa xam, odamlar osongina yodda qolishi uchun sodda parollar qo‘yishadi. Parollarda raqam va tinish belgilaridan foydalanish parolni xavfsizlik darajasini oshiradi. Parol buzuvchi dasturlar ichida lug‘at so‘zlardan foydalanadiganlari xam uchrab turadi, bunday dasturlar parollarni yenggib qo‘ymasligi uchun parol 12 va undan ko‘p raqam va belgidan iborat bo‘lishi tavsiya qilinadi.

Parollarni yanada ishonchli bo‘lishi uchun parollarni har ikki-uch oyda almashtirib turish kerak. Hech bo‘lmaganda uchta asosiy bank, pochta va ijitmoiy

tarmoqlardagi parollarni o‘zgartirib turish kerak. Ayniqsa ularni boshqa tizimlar uchun avtorizatsiya qilish uchun ishlatsangiz.

Parol menejerlari bilan ishlash xam tavsiya qilinadi. Bu dasturlar bizga tez tez o‘zgartirib turiluvchi parollarni saqlab yurish va yangi parollarni yaratishga bizga yordam beradi.

Foydalanilgan adabiyotlar

1. J. Blocki, M. Blum, and A. Datta, “Human computable passwords,” CoRR, vol. abs/1404.0024, 2014. [Online]. Available: http://arxiv.org/abs/1404.0024
2. KeePassXC Password Manager. Retrieved August 2, 2021, from https:// keepassxc.org.
3. Kurbanov, Sultanboy. (2022). Methods and models of surface formation in the process of three-dimensional modeling. Asian Journal of Research in Social Sciences and Humanities. 12. 272-280. 10.5958/2249-7315.2022.00187.3.