6 –TOM 2 – SON / 2023 - YIL / 15 - FEVRAL

AUTENTIFIKATSIYA VA IDENTIFIKATSIYA JARAYONIDA FOYDALANUVCHI AXBOROTIGA BO`LADIGAN TAHDIDLAR

Abdusamatova Shaxodat Xojiakbar qizi
Islom Karimov nomidagi TDTU Olmaliq filiali huzuridagi akademik litsey informatika va axborot texnologiyalari o`qituvchisi
tel: +998(93) 375 – 42 - 15 e-mail: abdusamatovashahodat@gmail.com,
Mannonov Asliddin Akbar o`g`li
Al Xorazimiy nomidagi TATU kiberxavsizlik fakulteti talabasi tel: +998(97) 960- 03 - 02, e-mail: asliddinmannonov0980@gmail.com .

Annotatsiya: *Ushbu maqolada autentifikatsiya va identifikatsiya jarayonida foydalanuvchini axborotiga bo`ladigan tahdidlar, ularni oldini olish strategiyalari tahlili keltirilgan.*

Kalit so`zlar: *autentifikatsiya, identifikatsiya, axborotga tahdid, foydalanuvchi axboroti, insayderlar, noma'lum foydalanuvchi.*

Katta hajimdagi ma'lumotlarni xotirasida saqlovchi serverlardan tortib oddiy foydalanuvchigacha o`z ma'lumotlarini xavfsiz va ishonchli saqlanishini istaydi. ***Shaxsiy ma'lumotlar yoki muhim ma'lumotlar*** - bu alohida shaxslar bilan bog'langan yoki bog'lanishi mumkin bo'lgan ma'lumotlar yoki ma'lumotlar. Masalan, shaxsning tug'ilgan sanasi, jinsiy istagi, qayerdaligi, dini, shuningdek, kompyuteringizning IP manzili yoki ushbu turdagi ma'lumotlarga tegishli metama'lumotlar kabi aniq ko'rsatilgan xususiyatlarni o'z ichiga oladi. Bundan tashqari, shaxsiy ma'lumotlar xulq-atvorga oid ma'lumotlar ko'rinishida ham ko'proq yashirin bo'lishi mumkin, masalan, ijtimoiy tarmoqlardan, bu shaxslar bilan bog'lanishi mumkin. Shaxsiy ma'lumotlar maxfiy retseptlar, moliyaviy ma'lumotlar yoki harbiy razvedka kabi boshqa sabablarga ko'ra nozik, qimmatli yoki muhim deb hisoblangan ma'lumotlarga qarama-qarshi qo'yilishi mumkin. Parollar kabi boshqa ma'lumotlarni himoya qilish uchun foydalaniladigan ma'lumotlar bu erda hisobga olinmaydi. Garchi bunday xavfsizlik choralari (parollar) maxfiylikka hissa qo'shishi mumkin,Ushbu ma'lumotlarga begona shaxslar, ruxsatsiz insayderlar va boshqa buzg`unchi shaxslarni kirishini olini olish maqsadida turli himoya tizimlarini ishlab chiqadi. Himoya tizimi begonalar uchun mustahkam, tasodifiy foydalanuvchilar uchun ishonchli va shu bilan birga ruxsat etilgan foydalanuvchi uchun ortiqcha muamolarni keltirib chiqarmasligi lozim. Foydalanuvchining ayni axborot yoki xizmatdan foydalanish huquqiga ega yoki ruxsat etilganini tekshirish autentifikatsiya jarayonida amalga oshiriladi.

Autentifikatsiya deganda shaxsning o'zi da'vo qilgan shaxs ekanligini bilish jarayoni tushuniladi. Kirishni boshqarish dasturi faqat avtorizatsiya qilingan(ayni axborotdan foydalanish huquqiga ega) shaxslarga tizimlardan foydalanishga yoki

autentifikatsiya qilishning ba'zi usullaridan foydalangan holda ma'lumotlarga kirishga ruxsat berish uchun mo'ljallangan. Hozirgi kunda qo`lanilayotgan yangi autentifikatsiya texnologiyalariga quyidagilar misol bo`la oladi:

– **Token :** identifikatsiya kartasiga o'xshash jismoniy qurilma, u bitta foydalanuvchining shaxsini tasdiqlash uchun mo'ljallangan.

– **Smart karta** : Kirish ruxsati va boshqa ma'lumotlar bilan formatlangan chipni o'z ichiga olgan kredit karta o'lchamidagi qurilma.

– **Biometrik autentifikatsiya** : Barmoq izlari, yuz yoki retinal tasvir kabi odamning o'ziga xos xususiyatlarini saqlangan o'rnatilgan profil bilan solishtirish orqali haqiqiylikni tekshirish.

Maxfiylik nuqtai nazaridan, atributlarga asoslangan autentifikatsiyadan foydalanish yaxshi yechim bo'ladi, bu foydalanuvchilarning atributlari, masalan, ularning do'stlari, millati, yoshi va boshqalarga asoslangan onlayn xizmatlardan foydalanish imkonini beradi va bu takror shu xizmatdan foydalanganda bir muncha qulayliklarni yaratadi. Atributlarga qarab foydalanilganda, ular asosan aniq shaxslarga tegishli bo'lishi mumkin, ammo bu endi hal qiluvchi ahamiyatga ega emas chunki bitta foydalanuvchi bir vaqtning o`zida bir nechda xizmztlardan foydalanayotgan bo`lishi, turli saytlarga a’zo bo`lishi mumkin, lekin ro`yxatdan o`tish vaqtida u o`zini turlicha tanishtirishi va o`zi haqidagi ma’lumotlarni oshkor qilishdagi ihtiyoriylik sabab tizimda bazan anglashilmovchiliklar ko`zga tashlanmoqda . Bundan tashqari, foydalanuvchilarni endi turli xizmatlar orqali kuzatib bo‘lmaydi, chunki ular turli xizmatlarga kirish uchun turli atributlardan foydalanishlari mumkin, bu esa bir nechta tranzaksiyalar bo‘yicha onlayn identifikatorlarni kuzatishni qiyinlashtiradi va shu tariqa foydalanuvchi uchun maxfiylik imkonini beradi. Shaxsiy ma'lumotlarni himoya qilish va boshqalar tomonidan ushbu ma'lumotlarga kirishni to'g'ridan-to'g'ri yoki bilvosita nazorat qilish autentifikatsiya va identifikatsiya jarayonlarining muhim omili hisoblanadi. Ushbu jarayondagi zaifliklar tufayli quyidagi ko`ngilsiz holatlar kelib chiqishi mumkin:

– **Foydalanuvchining shaxsi va shaxsiyati bilan bog`liq masalalar:** boshqa shaxslarning bank hisobiga, profiliga, ijtimoiy media hisobiga, bulutli omborlariga, xususiyatlariga va joylashgan joyiga cheksiz kirishi ma'lumotlar sub'ektiga turli yo'llar bilan zarar etkazish uchun ishlatilishi mumkin.

– **Axborot tengsizligi:** shaxsiy ma'lumotlar tovarga aylandi. Jismoniy shaxslar odatda o'z ma'lumotlaridan foydalanish bo'yicha shartnomalar bo'yicha muzokaralar olib borish uchun yaxshi holatda emaslar va sheriklar shartnoma shartlariga rioya qilishlarini tekshirish uchun vositalarga ega emaslar. Ma'lumotlarni himoya qilish bo'yicha qonunlar, tartibga solish va boshqaruv shaxsiy ma'lumotlarni uzatish va almashish bo'yicha shartnomalar tuzish uchun adolatli shart-sharoitlarni yaratishga va ma'lumotlar sub'ektlariga cheklar va muvozanatlar, zararni qoplash kafolatlari va shartnoma shartlariga rioya etilishini nazorat qilish vositalari bilan

ta'minlashga qaratilgan. Moslashuvchan narxlarni belgilash, narxlarni maqsadli belgilash va narxlarni o'lchash, dinamik muzokaralar odatda assimetrik ma'lumotlar va ma'lumotlarga kirishda katta nomutanosiblik asosida amalga oshiriladi. Shuningdek, marketingda tanlov modellashtirish, siyosiy kampaniyalarda mikro-targeting,

– **Axborot adolatsizligi va kamsitish:** Bir sohada yoki kontekstda (masalan, sog'liqni saqlash) taqdim etilgan shaxsiy ma'lumotlar boshqa sohada yoki kontekstda (masalan, tijorat operatsiyalarida) foydalanilganda uning ma'nosini o'zgartirishi va shaxs uchun kamsitish va kamchiliklarga olib kelishi mumkin.

– **Axloqiy avtonomiya va inson qadr-qimmatiga tajovuz:** Maxfiylikning yo'qligi odamlarni o'z tanlovlariga ta'sir qiladigan tashqi kuchlar ta'siriga olib kelishi va ularni boshqacha qabul qilmagan qarorlar qabul qilishga majbur qilishi mumkin. Ommaviy kuzatuv odamlar muntazam, tizimli va doimiy ravishda tanlov va qarorlar qabul qiladigan vaziyatga olib keladi, chunki ular boshqalar ularni kuzatayotganini bilishadi.

FOYDALANILGAN ADABIYOTLAR:

1. “Xavfsizlik va nazorat qilish uchun texnologiyalar va vositalar” vikipediya ma’lumoti

2. Stenford falsafa entsiklopediyasi “Maxfiylik va axborot texnologiyalari” 2014 yil 20-noyabr.

3. Jey Palter tomonidan “6 Jismoniy xavfsizlikning rivojlanayotgan tendentsiyalari”2021 yil 8-mart Jismoniy xavfsizlikda yurtilayotgan trendlar rukunida.

4. “Xavfsizlik texnologiyalari bo'yicha qo'llanma va 2022 yilgi tendentsiyalar” 2023 Openpath