Ikki bosqichli autentifikatsiya (2FA) va uni chetlab o‘tish usullari
Двухфакторная аутентификация (2FA) и способы её обхода
Two-factor authentication (2FA) and ways to bypass it

Behzod Sobirjonov Qahramonivich
FarDu Axborot tehnologiyalari
kafedrasi o‘qituvchisi
behzodbekqahramonovich@gmail.com
Muhammadjonova Mohiraxon Hamdamjon qizi
FarDu Axborot tizimlari va texnologiyalari
yo‘nalishi 2-bosqich talabasi
sumayyamuhammadjonova1@gmail.com
Telefon raqam:99-699-48-28

Annotatsiya: Ushbu maqolada zamonaviy axborot tizimlarida keng qo‘llanilayotgan ikki bosqichli autentifikatsiya (2FA) mexanizmi, uning ishlash prinsiplari hamda axborot xavfsizligini ta’minlashdagi o‘rni tahlil qilinadi. Shuningdek, 2FA tizimlarining amaliyotda uchraydigan zaifliklari, ularni chetlab o‘tish bilan bog‘liq zamonaviy tahdidlar va ushbu xavflarni kamaytirish yo‘llari ilmiy yondashuv asosida yoritiladi.

Kalit so‘zlar: Kiberxavfsizlik, 2FA, autentifikatsiya, OTP, phishing, xavfsizlik, tarmoq himoyasi

Аннотация: В статье рассматриваются принципы работы двухфакторной аутентификации (2FA), её значение для обеспечения информационной безопасности, а также анализируются существующие уязвимости и методы обхода данной технологии.

Ключевые слова: Кибербезопасность, 2FA, аутентификация, OTP, фишинг, защита информации

Abstract: This article analyzes the principles of Two-Factor Authentication (2FA), its importance in information security, and examines known vulnerabilities and bypass techniques. The study also outlines practical recommendations to mitigate associated risks.

Keywords: Cybersecurity, 2FA, authentication, OTP, phishing, security

KIRISH

Zamonaviy axborot jamiyatida raqamli xizmatlardan foydalanish hajmining ortib borishi bilan bir qatorda, foydalanuvchi ma’lumotlarini himoya qilish masalasi ham dolzarb ahamiyat kasb etmoqda. Internet tarmoqlari orqali amalga oshiriladigan moliyaviy operatsiyalar, shaxsiy yozishmalar va korporativ ma’lumotlar oddiy autentifikatsiya vositalari bilan yetarlicha himoyalanmaydi. An’anaviy parolga asoslangan tizimlar ko‘plab zaifliklarga ega bo‘lib, ularni buzish uchun zamonaviy kiberhujum usullari keng qo‘llanilmoqda.

Shu sababli autentifikatsiya jarayonini kuchaytirish maqsadida ikki bosqichli autentifikatsiya mexanizmi joriy etildi. Ushbu yondashuv foydalanuvchi shaxsini tasdiqlashda ikki xil omilni talab qiladi va bu orqali tizimga ruxsatsiz kirish ehtimolini sezilarli darajada kamaytiradi. 2FA texnologiyasi bugungi kunda bank tizimlari, ijtimoiy tarmoqlar, elektron pochta xizmatlari hamda korporativ infratuzilmalarda keng qo‘llanilmoqda.

Ikki bosqichli autentifikatsiya jarayonida foydalanuvchi avvalo o‘z login va parolini kiritadi, so‘ngra tizim tomonidan taqdim etilgan qo‘shimcha tasdiqlash bosqichidan o‘tadi. Bu tasdiqlash

ko‘pincha mobil qurilmaga yuborilgan bir martalik kod, maxsus autentifikator ilova yoki biometrik ma’lumotlar orqali amalga oshiriladi. Ushbu mexanizm parol o‘g‘irlangan taqdirda ham hisobni himoya qilish imkonini beradi.

2FA ning muhim afzalliklaridan biri shundaki, u turli xil kiberhujumlarga qarshi qo‘shimcha himoya qatlamini yaratadi. Ayniqsa, parolni taxmin qilish yoki ma’lumotlar bazasidan o‘g‘irlash orqali amalga oshiriladigan hujumlar ushbu mexanizm orqali sezilarli darajada cheklanadi. Shu bilan birga, autentifikatsiya jarayonining har bir bosqichida qo‘llaniladigan kriptografik usullar tizim xavfsizligini yanada mustahkamlaydi.

Shunga qaramay, 2FA mutlaq xavfsizlikni kafolatlamaydi. So‘nggi yillarda olib borilgan tadqiqotlar shuni ko‘rsatadiki, ayrim hollarda ushbu mexanizmni ham chetlab o‘tish mumkin. Bunday zaifliklar asosan inson omili, noto‘g‘ri konfiguratsiya yoki texnik kamchiliklar bilan bog‘liq. Masalan, foydalanuvchini aldash orqali uning autentifikatsiya ma’lumotlarini qo‘lga kiritish keng tarqalgan usullardan biri hisoblanadi.

Zamonaviy kiberhujumlarda real vaqt rejimida amalga oshiriladigan fishing texnologiyalari orqali foydalanuvchi nafaqat parolini, balki vaqtinchalik tasdiqlash kodini ham hujumchiga o‘zi taqdim etishi mumkin. Bundan tashqari, mobil aloqa infratuzilmasidagi zaifliklardan foydalanib, telefon raqamini boshqa SIM kartaga ko‘chirish orqali SMS orqali yuboriladigan kodlarni qo‘lga kiritish holatlari ham kuzatilmoqda.

Boshqa tomondan, zararli dasturiy ta’minot foydalanuvchi qurilmasiga o‘rnatilib, autentifikatsiya jarayonini kuzatishi yoki maxfiy ma’lumotlarni uzatishi mumkin. Ayrim hollarda esa foydalanuvchi tizimga muvaffaqiyatli kirgandan so‘ng uning sessiyasi o‘g‘irlanadi va bu orqali qo‘shimcha tekshiruv bosqichlari chetlab o‘tiladi. Bu kabi holatlar 2FA tizimining faqat texnik emas, balki tashkiliy va insoniy omillarga ham bog‘liqligini ko‘rsatadi.

Ikki bosqichli autentifikatsiyaning samaradorligi uni to‘g‘ri joriy etish va foydalanish darajasiga bevosita bog‘liq. Ayniqsa, SMS asosidagi tasdiqlash usuli boshqa variantlarga nisbatan nisbatan zaifroq hisoblanadi. Shu sababli autentifikator ilovalar yoki apparat tokenlardan foydalanish yanada ishonchli yechim sifatida tavsiya etiladi.

Xulosa

Ikki bosqichli autentifikatsiya (2FA) zamonaviy raqamli xavfsizlikning ajralmas qismi bo‘lib, u oddiy parolga qo‘shimcha ravishda foydalanuvchi shaxsini tasdiqlovchi ikkinchi bir "himoya qatlami"ni qo‘shadi. Bu usul foydalanuvchining paroli o‘g‘irlangan taqdirda ham, hisobga kirish uchun maxsus SMS kod, autentifikator ilovasi (masalan, Google Authenticator) yoki biometrik ma’lumotlarni talab qilish orqali kiberjinoyatchilarga to‘siq bo‘ladi.

Biroq, 2FA tizimi mutlaq yengilmas emas va tajovuzkorlar uni chetlab o‘tishning bir qancha hiylakor usullarini ishlab chiqqanlar. Eng keng tarqalgan usullardan biri bu "Session Hijacking" (sessiyani o‘g‘irlash) bo‘lib, bunda xakerlar brauzerdagi kuki (cookies) fayllarini qo‘lga kiritish orqali tizimni foydalanuvchi allaqachon login va 2FA-dan o‘tgan deb o‘ylashga majbur qiladilar. Shuningdek, "SIM swapping" deb ataluvchi usulda jinoyatchilar aloqa operatorini aldab, foydalanuvchining telefon raqamini o‘zining SIM-kartasiga ko‘chirib olishadi va barcha SMS kodlarni to‘g‘ridan-to‘g‘ri qabul qilishadi.

Yana bir zamonaviy tahdid — bu "MFA Fatigue" (autentifikatsiya toliqishi) deb ataladigan hujumdir. Bunda tajovuzkor foydalanuvchi telefoniga tinimsiz tasdiqlash so‘rovlarini yuboraveradi, natijada charchagan yoki adashgan foydalanuvchi "tasdiqlash" tugmasini bosib yuboradi. Shuningdek, soxta saytlar orqali foydalanuvchidan ham parolni, ham 2FA kodini real vaqt rejimida

yig‘ib oluvchi murakkab fishinq hujumlari ham mavjud. Shunga qaramay, 2FA-dan foydalanish uni ishlatmaslikdan ko‘ra o‘n baravar xavfsizroqdir, chunki u aksariyat avtomatlashtirilgan hujumlarni samarali to‘xtatib qoladi.

Foydalanilgan adabiyotlar

1. Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2012).
The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. IEEE Symposium on Security and Privacy,
2. NIST. (2017).
Digital Identity Guidelines (SP 800-63-3). National Institute of Standards and Technology. https://pages.nist.gov/800-63-3/
3. OWASP Foundation. (2021).
Authentication Cheat Sheet. https://owasp.org/www-project-cheat-sheets/cheatsheets/Authentication_Cheat_Sheet.html
4. Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017).
Digital Identity Guidelines: Authentication and Lifecycle Management. NIST Special Publication 800-63B.
5. SANS Institute. (2020).
Multi-Factor Authentication: Threats and Best Practices. https://www.sans.org/white-papers/
pages.nist.gov (https://pages.nist.gov/800-63-3/)
NIST SP 800-63 Digital Identity Guidelines
NIST Special Publication 800-63 Digital Identity Guidelines