KIBERXAVFSIZLIKDA IKKI BOSQICHLI AUTENTIFIKATSIYA (2FA) VA UNI CHETLAB O‘TISH USULLARI

ИСПОЛЬЗОВАНИЕ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ (2FA) И МЕТОДЫ ЕЁ ОБХОДА В КИБЕРБЕЗОПАСНОСТИ

APPLICATION OF TWO-FACTOR AUTHENTICATION (2FA) AND METHODS OF BYPASSING IT IN CYBERSECURITY

Sobirjonov Behzod Qaxramon o‘g‘li
Farg‘ona davlat universiteti Axborot texnologiyalari kafedrasio‘qituvchisi
behzodbekqahramonovich@gmail.com
Muhammadaliyev Sirojiddin Zaylobiddin o‘g‘li
Farg‘ona davlat universiteti Axborot tizimlari va texnologiyalar yo‘nalishi
2-kurs talabasi
sirojiddinmuhammadaliyev8@gmail.com
https://doi.org/10.5281/zenodo.19909523

ANNOTATSIYA. Ushbu maqolada kiberxavfsizlik tizimlarida keng qo‘llaniladigan ikki bosqichli autentifikatsiya (2FA) mexanizmi, uning ishlash prinsiplari va ahamiyati tahlil qilinadi. Shuningdek, 2FA tizimini chetlab o‘tish usullari nazariy jihatdan ko‘rib chiqilib, ularning xavfsizlikka ta’siri yoritiladi. Zamonaviy tahdidlar va hujum usullari asosida autentifikatsiya jarayonlarini mustahkamlash bo‘yicha tavsiyalar beriladi. Maqola axborot tizimlarining himoyasini kuchaytirish va foydalanuvchi ma’lumotlarini ishonchli saqlashga qaratilgan.

АННОТАЦИЯ. В данной статье рассматривается механизм двухфакторной аутентификации (2FA), широко применяемый в системах кибербезопасности, его принципы работы и значение. Также анализируются теоретические методы обхода 2FA и их влияние на безопасность информационных систем. На основе современных угроз и атак предлагаются рекомендации по усилению процессов аутентификации. Статья направлена на повышение уровня защиты информационных систем и обеспечение безопасности пользовательских данных.

ABSTRACT. This article examines the mechanism of two-factor authentication (2FA), which is widely used in cybersecurity systems, its working principles, and its importance. The paper also analyzes theoretical methods of bypassing 2FA and their impact on information security. Based on modern threats and attack techniques, recommendations are provided to strengthen authentication processes. The study aims to enhance the protection of information systems and ensure the security of user data.

Kalit so‘zlar. Ikki bosqichli autentifikatsiya (2FA), kiberxavfsizlik, autentifikatsiya mexanizmlari, xavfsizlik zaifliklari, identifikatsiya va verifikatsiya, phishing hujumlari, ijtimoiy muhandislik, bir martalik parol (OTP), ma’lumotlar himoyasi, axborot xavfsizligi

Ключевые слова. Двухфакторная аутентификация (2FA), кибербезопасность, механизмы аутентификации, уязвимости безопасности, идентификация и верификация, фишинговые атаки, социальная инженерия, одноразовый пароль (OTP), защита данных, информационная безопасность

Keywords. Two-factor authentication (2FA), cybersecurity, authentication mechanisms, security vulnerabilities, identification and verification, phishing attacks, social engineering, one-time password (OTP), data protection, information security

Kirish.

Bugungi kunda raqamli texnologiyalarning jadal rivojlanishi bilan bir qatorda kiberxavfsizlik masalalari ham dolzarb ahamiyat kasb etmoqda. Axborot tizimlari, onlayn xizmatlar va mobil ilovalarning keng qo‘llanilishi foydalanuvchi ma’lumotlarini himoya qilish zaruratini yanada kuchaytirdi. Ayniqsa, shaxsiy ma’lumotlar, moliyaviy axborotlar va maxfiy tizimlarga ruxsatsiz kirish holatlari ortib borayotgan bir vaqtda, ishonchli autentifikatsiya mexanizmlarini joriy etish muhim vazifalardan biri hisoblanadi.

Ikki bosqichli autentifikatsiya (2FA) ushbu muammoning samarali yechimlaridan biri sifatida keng qo‘llanilmoqda. Ushbu usul foydalanuvchini tasdiqlashda ikki xil omilga asoslanadi va oddiy parolga nisbatan yuqori darajadagi xavfsizlikni ta’minlaydi. Biroq, zamonaviy kiberhujumlar rivojlanib borayotganligi sababli, 2FA tizimlarini chetlab o‘tishga qaratilgan turli usullar ham paydo bo‘lmoqda.

Mazkur maqolada ikki bosqichli autentifikatsiya tizimining ishlash prinsiplari, uning afzalliklari hamda mavjud zaifliklari tahlil qilinadi. Shuningdek, 2FA ni chetlab o‘tishning nazariy jihatlari ko‘rib chiqilib, axborot tizimlari xavfsizligini yanada mustahkamlash bo‘yicha taklif va tavsiyalar beriladi.

Mazkur amaliy ishda ikki bosqichli autentifikatsiya (2FA) tizimlarining ishlash prinsiplari hamda ularning xavfsizlik darajasi tahlil qilindi. 2FA tizimi foydalanuvchini tasdiqlashda ikki xil omildan foydalanadi, ya’ni foydalanuvchi avval login va parol orqali tizimga kirishga harakat qiladi, so‘ngra qo‘shimcha ravishda bir martalik tasdiqlash kodi kiritiladi. Ushbu kod odatda SMS xabar, maxsus mobil ilova yoki apparat token orqali yuboriladi.

Tahlil jarayonida autentifikatsiya bosqichlari ketma-ketligi o‘rganildi. Dastlab foydalanuvchi tomonidan kiritilgan login va parol server tomonidan tekshirildi. Agar ma’lumotlar to‘g‘ri bo‘lsa, tizim tomonidan ikkinchi bosqich – ya’ni bir martalik parol (OTP) yuborildi. Ushbu kod foydalanuvchi tomonidan kiritilgach, tizimga kirish ruxsati berildi. Shu orqali 2FA tizimi oddiy autentifikatsiyaga nisbatan yuqori darajadagi xavfsizlikni ta’minlashi kuzatildi.

Amaliy ish davomida 2FA tizimlaridagi ayrim zaifliklar ham tahlil qilindi. Jumladan, agar tizimda noto‘g‘ri kiritilgan kodlar soniga cheklov qo‘yilmagan bo‘lsa, hujumchi ko‘p marotaba urinish orqali to‘g‘ri kodni aniqlashi mumkinligi aniqlandi. Bundan tashqari, fishing (phishing) hujumlari orqali foydalanuvchilarning login, parol va 2FA kodlarini qo‘lga kiritish ehtimoli mavjudligi o‘rganildi.

Shuningdek, sessiyani o‘g‘irlash (session hijacking) holatlari ham tahlil qilindi. Agar foydalanuvchi tizimga muvaffaqiyatli kirgandan so‘ng uning sessiya identifikatori uchinchi shaxs tomonidan qo‘lga kiritilsa, 2FA bosqichini qayta bosib o‘tmasdan tizimga kirish imkoniyati yuzaga kelishi mumkin. Bu esa tizim xavfsizligiga jiddiy tahdid soladi.

Yana bir muhim jihat sifatida SMS asosidagi autentifikatsiya tizimlarining zaif tomonlari ko‘rib chiqildi. Xususan, SIM-karta almashtirish (SIM swap) hujumi orqali hujumchi foydalanuvchining telefon raqamini o‘z nazoratiga olib, yuborilgan tasdiqlash kodlarini qabul qilishi mumkin. Bu esa 2FA tizimining ishonchliligini pasaytiradi.

O‘tkazilgan tahlillar natijasida shunday xulosaga kelindiki, ikki bosqichli autentifikatsiya tizimi yuqori darajadagi himoyani ta’minlashiga qaramasdan, noto‘g‘ri sozlangan yoki yetarlicha himoyalanmagan holatlarda turli kiberhujumlarga nisbatan zaif bo‘lishi mumkin. Shu sababli autentifikatsiya tizimlarida qo‘shimcha himoya choralarini qo‘llash, xususan, urinishlar sonini cheklash, foydalanuvchilarni fishing hujumlari haqida ogohlantirish hamda zamonaviy autentifikatsiya usullaridan foydalanish muhim ahamiyat kasb etadi.

XULOSA

Mazkur maqolada kiberxavfsizlik tizimlarida muhim ahamiyatga ega bo‘lgan ikki bosqichli autentifikatsiya (2FA) mexanizmi atroflicha tahlil qilindi. Tadqiqot davomida 2FA ning ishlash prinsiplari, uning an’anaviy parol asosidagi autentifikatsiyaga nisbatan ustunliklari hamda zamonaviy axborot tizimlarida tutgan o‘rni yoritib berildi.

Shu bilan birga, 2FA tizimlarining ayrim zaif tomonlari ham ko‘rib chiqildi. Xususan, bruteforce hujumlari, fishing usullari, sessiyani o‘g‘irlash va SIM-karta orqali amalga oshiriladigan hujumlar kabi xavflar mavjudligi aniqlandi. Bu esa 2FA tizimlari mutlaq xavfsizlikni ta’minlamasligini, balki ularni to‘g‘ri sozlash va qo‘shimcha himoya choralarini qo‘llash zarurligini ko‘rsatadi.

O‘rganishlar natijasida shunday xulosaga kelish mumkinki, ikki bosqichli autentifikatsiya axborot xavfsizligini sezilarli darajada oshiradi, biroq zamonaviy kiberxavflarga qarshi kurashishda uni yanada takomillashtirish talab etiladi. Shu sababli, autentifikatsiya jarayonlarini kuchaytirish, foydalanuvchilarni xabardor qilish va ilg‘or xavfsizlik texnologiyalaridan foydalanish muhim vazifa hisoblanadi.

Adabiyotlar, References, Литературы:

1. Stallings W. — Network Security Essentials: Applications and Standards. Pearson Education, 2017.
2. Kaufman C., Perlman R., Speciner M. — Network Security: Private Communication in a Public World. Prentice Hall, 2016.
3. NIST — Digital Identity Guidelines (SP 800-63). National Institute of Standards and Technology, 2020.
4. OWASP Foundation — Authentication Cheat Sheet. https://owasp.org
5. Bonneau J. et al. — The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. IEEE Symposium on Security and Privacy, 2012.