ANALYSIS OF SOCIAL ENGINEERING ATTACKS

IJTIMOIY INJENERIYADA HUJUMLAR TAHLILI

Dottoyev Sayfulla Khamidullayevich
Associate professor, Tashkent state pedagogical university

Annotation: *This thesis explores the phenomenon of social engineering attacks, including their historical evolution, common techniques, consequences, and preventive measures. Social engineering exploits human psychology to extract sensitive information or gain unauthorized access. The study explains the effectiveness of these attacks by their reliance on emotions such as fear, urgency, and curiosity. Understanding the tactics used in social engineering and implementing robust security practices can significantly reduce the vulnerability of individuals and organizations to such threats.*

Keywords: *social engineering, phishing, pretexting, cybersecurity, human manipulation.*

Annotatsiya *Ushbu tezisda ijtimoiy muhandislik hujumlari hodisasini, ularning tarixiy evolyutsiyasi, keng tarqalgan usullari, oqibatlari va oldini olish choralarini o‘rganadi. Ijtimoiy muhandislik nozik ma’lumotlarni oshkor qilish yoki ruxsatsiz kirish huquqini berish uchun inson psixologiyasidan foydalanadi. Tadqiqot ushbu hujumlarning samaradorligini ularning qo‘rquv, shoshilinchlik va qiziqish kabi insoniy his-tuyg‘ularga tayanishi bilan izohlaydi. Ijtimoiy muhandislikda qo‘llaniladigan taktikalarni tushunish va mustahkam xavfsizlik amaliyotlarini joriy etish orqali shaxslar va tashkilotlar bunday tahdidlarga chalinish xavfini sezilarli darajada kamaytirishi mumkin.*

Kalit so‘zlar: *ijtimoiy muhandislik, fishing, pretexting, kiberxavfsizlik, insoniy manipulyatsiya.*

Ijtimoiy muhandislik - bu ma’lumot yoki tizimlarga ruxsatsiz kirish huquqini olish uchun inson ishonchi va zaif tomonlaridan foydalanadigan psixologik manipulyatsiya shakli. Texnik kiberhujumlardan farqli o‘laroq, ijtimoiy muhandislik inson omiliga qaratilgan bo‘lib, raqamli davrda doimiy rivojlanib boruvchi tahdid hisoblanadi. Ushbu maqolada ijtimoiy muhandislikning tarixi, keng tarqalgan hujum usullari, ularning oqibatlari va ularning oldini olish bo‘yicha tavsiyalar muhokama qilinadi.

Ushbu tadqiqotning dolzarbligi ijtimoiy muhandislik hujumlarining tobora murakkablashib borayotganligida va ularning butun dunyo bo‘ylab shaxslar va tashkilotlar uchun katta xavf tug‘dirishida namoyon bo‘ladi. Ushbu hujumlarni tushunish samarli himoya strategiyalarini ishlab chiqish uchun juda muhimdir.

Ijtimoiy muhandislik qadim zamonlardan boshlab uzoq tarixga ega. "Ijtimoiy muhandislik" atamasi birinchi marta 19-asr oxirida gollandiyalik sanoatchi J.C. Van Marken tomonidan sanoat sharoitida insoniy muammolarni hal qilishni tasvirlash uchun

ishlatilgan. 20-asr boshlarida sotsiolog Edvard L. Earp ijtimoiy muammolarga muhandislik tamoyillarini qo‘lladi va jamiyat muammolariga tahliliy yondashuvni ta’kidladi.

Raqamli davr ijtimoiy muhandislikni kiberxavfsizlik tahdidiga aylantirdi. Kompyuterlar va internetning paydo bo‘lishi bilan hujumchilar texnik himoyani chetlab o‘tish uchun psixologik manipulyatsiyadan foydalana boshladilar. Zamonaviy ijtimoiy muhandislik hujumlari, masalan, fishing va pretexting, juda maqsadli va aniqlash qiyin bo‘lgan hujumlardir.

Keng tarqalgan ijtimoiy muhandislik usullari

1. Fishing: Qurbonlarni zararli havolalar yoki biriktirmalarni bosishga undash uchun mo‘ljallangan yolg‘on elektron pochta yoki xabarlar.
2. Pretexting: Nozik ma’lumotlarni olish uchun soxta stsenariy yaratish (masalan, IT yordamchisini o‘ynash).
3. Baiting: Zararli dasturlarni yuklab olishga undash uchun qiziqarli takliflar (masalan, bepul dasturiy ta’minot).
4. Quid Pro Quo: Ma’lumot yoki kirish huquqi evaziga foyda taklif qilish.
5. Tailgating: Ruxsatsiz shaxslarning tegishli ruxsatga ega bo‘lgan shaxslarga ergashib, jismoniy kirish huquqini olish.

Ijtimoiy muhandislik hujumlarining oqibatlari: Moliyaviy yo‘qotishlar: Firibgarlik faoliyati uchun shaxsiy yoki moliyaviy ma’lumotlarning o‘g‘irlanishi. Ma’lumotlar buzilishi: Mijoz yozuvlari yoki intellektual mulk kabi nozik ma’lumotlarning oshkor etilishi. Obro‘ga putur yetkazish: Xavfsizlik buzilishi tufayli ishonch va brend imijining yo‘qolishi. Operatsion uzilishlar: Zararli dasturiy ta’minot hujumlari yoki tizim blokirovkalari tufayli biznes faoliyatining to‘xtab qolishi.

Profilaktika choralari

Xavfsizlik bo‘yicha o‘qitish: Xodimlar va shaxslarni ijtimoiy muhandislikning keng tarqalgan usullari haqida o‘qitish.

Keluvchi so‘rovlarni tekshirish: Havolalar bosish yoki ma’lumot almashishdan oldin jo‘natuvchining shaxsini tasdiqlash.

Kuchli parollar va MFA: Murakkab parollardan foydalanish va ko‘p faktorli autentifikatsiyani yoqish.

Yuklab olishda ehtiyot bo‘lish: Faqat ishonchli manbalardan fayllarni yuklab olish.

Shubhali faoliyat haqida xabar berish: Har qanday shubhali elektron pochta, qo‘ng‘iroq yoki xabarlar haqida tegishli organlarga xabar berish.

Xulosa

Ijtimoiy muhandislik hujumlari inson psixologiyasiga tayanishi tufayli raqamli dunyoda jiddiy tahdid bo‘lib qolmoqda. Fishing va pretexting kabi usullar qo‘rquv va qiziqish kabi his-tuyg‘ulardan foydalangan holda texnik himoyani chetlab o‘tadi. Biroq, xabardorlik, ta’lim va mustahkam xavfsizlik amaliyotlari orqali shaxslar va tashkilotlar ushbu xavflarni kamaytirishi mumkin. Doimiy hushyorlik va rivojlanayotgan taktikalarga moslashish tobora o‘sib borayotgan raqamli dunyoda xavfsizlikni saqlab qolish uchun juda muhimdir.

FOYDALANILGAN ADABIYOTLAR

1. Xusanov, N. (2022). “Ijtimoiy injeneriya va uning xavflari”, Axborot texnologiyalari va xavfsizlik jurnali, №3, 45–49.
2. Mitnick, K. D., & Simon, W. L. (2011). The Art of Deception: Controlling the Human Element of Security. Wiley.
3. Conteh, N. Y., & Schmick, P. J. (2016). “Cybersecurity: Attacks and Defenses.” International Journal of Computer and Information Technology, 5(9), 876–882.
4. Sayfulla, Dottoyev. "Information and methodological support-as a means of intensifying the educational process. Euro-Asia Conferences, 159-161." 2021
5. Fayzieva Makhbuba Rakhimjonovna. (2024). Organization of education in the conditions of digital transformation. Ethiopian International Mul-tidisciplinary Research Conferences, 1(2), 98–100. Retrieved from https://eijmr.org/conferences/index.php/eimrc/article/view/147
6. Rahimjonovna F. M., Xamidullayevich D. S. Raqamli ta’lim texnologiyalari va ularning bugungi kundagi ahamiyati //Miasto Przyszłości. – 2024. – T. 49. – C. 1171-1175.