INSON OMILI VA IJTIMOIY MUHANDISLIK: KIBERXAVFSIZLIK TIZIMLARIDAGI ZAIFLIKLARNING EVOLYUTSION TAHLIL

Muxtoraliyeva Nozima Shuxratovna
ISFT Samarqand

Annotatsiya. Maqola inson omili va ijtimoiy muhandislikning kiberxavfsizlik tizimlaridagi zaifliklarga ta'sirini evolyutsion tahlil qiladi. Kiberxavfsizlik sohasida texnologik yechimlar muhim bo'lsa-da, inson xatti-harakatlari va psixologik zaifliklar ko'pincha kiberhujumlarning asosiy sababi hisoblanadi. Ijtimoiy muhandislik usullari orqali kiberjinoyatchilar foydalanuvchilarni manipulyatsiya qilib, tizimlarga kirishni ta'minlaydilar. Maqolada kiberhujumlarning evolyutsiyasi, inson omilining roli va kelajakdagi xavf-xatarlarni boshqarish strategiyalari haqida fikr yuritiladi. Foydalanuvchilarni ta'lim berish va xavfsizlik madaniyatini rivojlantirish zarurligi ta'kidlanadi, shuningdek, ilg'or texnologiyalarni qo'llash orqali kiberxavfsizlikni mustahkamlash yo'llari ko'rsatiladi.

Kalit so‘zlar: Inson omili, Ijtimoiy muhandislik, Kiberxavfsizlik, Zaifliklar, Evolyutsion tahlil, Kiberhujumlar, Foydalanuvchi xatti-harakatlari

KIRISH.

Kiberxavfsizlik sohasida inson omili va ijtimoiy muhandislikning o'rni juda katta. Kiberxavfsizlik tizimlari, odatda, texnologik yechimlar va protokollarga asoslangan bo'lsa-da, inson omili ko'pincha zaifliklar va kiberhujumlarning asosiy sababi bo'lib qoladi. Ushbu maqolada inson omili va ijtimoiy muhandislikning kiberxavfsizlik tizimlaridagi zaifliklarga ta'siri evolyutsion jihatdan tahlil qilinadi. Kiberxavfsizlik tizimlarining samaradorligi ko'pincha insonlarning xatti-harakatlari va qarorlariga bog'liq. Odamlar kiberxavfsizlik protokollarini to'g'ri tushunmasligi yoki ularga amal qilmasligi natijasida tizimlar zaiflashadi. Masalan, parolni kuchli tanlash, ikki faktorli autentifikatsiya va phishing xujumlariga qarshi ehtiyotkorlik kabi oddiy qoidalar ko'plab foydalanuvchilar tomonidan e'tiborsiz qoldiriladi. Ijtimoiy muhandislik — bu insonlarni manipulyatsiya qilish orqali ma'lumotlarga yoki tizimlarga kirishni ta'minlaydigan usuldir. Kiberjinoyatchilar ko'pincha foydalanuvchilarning psixologik zaifliklaridan foydalanadilar. Ular ishonchli manbalar sifatida o'zlarini ko'rsatib, ma'lumotlarni olish uchun foydalanuvchilarni aldashadi. Bu jarayon, ko'pincha, odamlarning tabiiy ishonchidan foydalanish orqali amalga oshiriladi. Kiberxavfsizlik tizimlaridagi zaifliklar vaqt o'tishi bilan evolyutsiyaga uchraydi. Dastlabki kiberhujumlar oddiy phishing xujumlari bilan boshlanib, keyinchalik murakkab va noaniq usullar bilan davom etmoqda. Bugungi kunda,

kiberjinoyatchilar sun'iy intellekt va mashina o'rganish kabi ilg'or texnologiyalarni qo'llash orqali hujumlarini yanada kuchaytirmoqdalar.

Evolyutsion tahlil shuni ko'rsatadiki, kiberhujumlar faqat texnologik jihatga emas, balki inson psixologiyasiga ham bog'liqdir. Misol uchun, COVID-19 pandemiyasi davrida masofadan ishlashning kengayishi ijtimoiy muhandislik hujumlariga yangi imkoniyatlar yaratdi. Foydalanuvchilar uyda ishlayotgan paytda, kiberjinoyatchilar ularning ehtiyotkorligini pasaytirishdan foydalanib, ko'proq muvaffaqiyatli hujumlar amalga oshirdilar. Kiberxavfsizlik strategiyalarini ishlab chiqishda inson omilini hisobga olish juda muhimdir. Tizimlar nafaqat texnologik jihatdan mustahkam bo'lishi, balki foydalanuvchilarning xatti-harakatlarini ham o'rganishi kerak. Bu jarayonda ta'lim va ongli ravishda xavf-xatarlarni boshqarish muhim ahamiyatga ega. Foydalanuvchilarni kiberxavfsizlik bo'yicha muntazam ravishda o'qitish, ularga xavflarni tushuntirish va ehtiyotkorlikni oshirish kiberhujumlarning oldini olishda samarali usuldir. Shuningdek, tashkilotlar ichida xavfsizlik madaniyatini rivojlantirish ham muhimdir. Bu madaniyat foydalanuvchilarni xavfsizlikka mas'uliyatli yondashishga undaydi.

Kiberxavfsizlik sohasida kelajakdagi yo'nalishlardan biri inson omilini yanada chuqurroq o'rganishdir. Sun'iy intellekt va analitik vositalar yordamida foydalanuvchilarning xatti-harakatlarini kuzatish va ularga mos ravishda xavfsizlik chora-tadbirlarini taklif qilish mumkin. Bunday yondashuvlar kiberxavfsizlik tizimlarining samaradorligini oshirishga yordam beradi. Shuningdek, ijtimoiy muhandislik tahdidlariga qarshi kurashishda zamonaviy texnologiyalarni qo'llash muhimdir. Masalan, avtomatik phishing aniqlash tizimlari yoki foydalanuvchi xatti-harakatlarini tahlil qiluvchi algoritmlar yordamida potentsial tahdidlarni oldindan aniqlash mumkin. Inson omili va ijtimoiy muhandislik kiberxavfsizlik tizimlaridagi zaifliklarning asosiy manbai hisoblanadi. Ularning evolyutsion tahlili kiberhujumlarning murakkabligini va inson psixologiyasining rolini ochib beradi. Kiberxavfsizlik strategiyalarini ishlab chiqishda foydalanuvchilarni ta'lim berish va xavfsizlik madaniyatini rivojlantirish zarurati mavjud. Kelajakda texnologik yechimlar bilan birga inson omilini hisobga olish kiberxavfsizlikni yanada mustahkamlashga yordam beradi. Ijtimoiy muhandislik - bu texnik vositalar emas, balki inson psixologiyasidan foydalanish orqali maxfiy ma’lumotlarni qo‘lga kiritish san’atidir. Hujumchilar insonning tabiiy xususiyatlarini - ishonch, qo‘rquv, qiziquvchanlik va yordam berish istagini - qurol sifatida ishlatadilar. Psixologik manipulyatsiyaning asosiy mexanizmlari:

1. **Avtoritetga bo‘ysunish:** Hujumchi o‘zini yuqori lavozimli shaxs (masalan, IT direktor yoki bank xodimi) sifatida ko‘rsatadi.

2. **Shoshilinchlik (Urgency):** "Hisobingiz bloklandi, darhol tasdiqlang!" kabi xabarlar insonni mantiqiy fikrlashdan chalg‘itib, hissiyotga berilishga majbur qiladi.

3. **Kamchilik hissi (Scarcity):** Cheklangan imkoniyatlar taklif qilish orqali foydalanuvchini shoshilinch qaror qabul qilishga undash.

Zaifliklarning evolyutsion rivojlanishi

Ijtimoiy muhandislik metodlari vaqt o‘tishi bilan sezilarli darajada murakkablashib bormoqda. Ularni bir necha bosqichga ajratish mumkin: Ilk bosqichlarda hujumchilar telefon orqali (vishing) yoki qog‘oz ko‘rinishidagi soxta hujjatlar bilan ishlashgan. Bu davrda asosiy maqsad suhbatdoshning diqqatini chalg‘itish va ma’lumotlarni "o‘g‘irlash" edi. Internetning ommalashishi bilan hujumlar elektron pochtaga ko‘chdi. Phishing (fishing) usuli orqali millionlab foydalanuvchilarga bir xil xat yuborish orqali "kattaroq to‘r" tashlash imkoniyati paydo bo‘ldi. Bu davrda soxta veb-sahifalar va linklar asosiy qurolga aylandi. Hujumchilar umumiy xatlardan voz kechib, aniq bir shaxs yoki kompaniyani nishonga olishni boshladilar. Bu bosqichda ijtimoiy tarmoqlar orqali olingan ma’lumotlar (ish joyi, qiziqishlar, do‘stlar ro‘yxati) o‘rganiladi va shaxsga moslashtirilgan, juda ishonchli xabarlar yuboriladi. Bugungi kunda evolyutsiya yangi bosqichga chiqdi. Sun’iy intellekt (AI) yordamida tovushni va videoni taqlid qilish (Deepfake) imkoniyati paydo bo‘ldi. Endilikda hujumchi rahbarining ovozi yoki video muloqotini yaratib, xodimlardan pul o‘tkazishni yoki maxfiy parollarni talab qilishi mumkin. Bu endi shunchaki "soxta xat" emas, balki "haqiqiy ko‘ringan yolg‘on"dir. Texnik tizimlar inson xatosini aniqlashda ko‘pincha ojiz qoladi. Masalan, agar foydalanuvchi o‘z parolini soxta saytga o‘zi kiritib bersa, tizim buni "legitim kirish" deb qabul qiladi. Shuning uchun, kiberxavfsizlik strategiyalari faqatgina firewall’larni kuchaytirishga emas, balki "Zero Trust" (Hech kimga ishonma) tamoyiliga asoslanishi kerak. Inson omili bilan kurashish uchun ikki yo‘nalishda ish olib borilishi shart:

1. **Texnik himoya:**

- Multi-factor Authentication (MFA) - paroldan tashqari qo‘shimcha tasdiqlash.
- AI asosidagi anomaliyalarni aniqlash tizimlari (oddiy foydalanuvchi harakatidan farq qiluvchi harakatlarni darhol bloklash).
- Email filtrlash va phishingga qarshi avtomatik skanerlash.

2. **Ijtimoiy-psixologik himoya (Security Awareness Training):**

- Xodimlarning kiber-savodxonligini oshirish.
- Doimiy simulyatsiya hujumlari (o‘quv maqsadida soxta phishing xabarlarini yuborish).
- Korporativ madaniyat shakllantirish: "Shubhali holatda tekshirish" qoidasini o‘rnatish. Kiberxavfsizlik - bu faqatgina kompyuter dasturlari bilan bog‘liq jarayon emas, balki inson psixologiyasi va texnologiya o‘rtasidagi muvozanatdir. Ijtimoiy muhandislik evolyutsiyasi ko‘rsatib berganidek, hujumchilar texnik to‘siqlarni aylanib o‘tish uchun insonning zaif nuqtalarini izlayveradi. Shuning uchun, kelajakdagi kiberxavfsizlik tizimlari nafaqat algoritmlarga, balki inson xatti-harakatlarini tahlil

qiluvchi va foydalanuvchini tayyorlovchi kompleks tizimlarga asoslanishi shart. Eng kuchli firewall’dan ko‘ra, kiber-savodxon xodim tizimni yaxshiroq himoya qilishi mumkin.

XULOSA.

Xulosa qilib aytganda, kiberxavfsizlik muammosining markazida texnologik kamchiliklar emas, balki inson psixologiyasiga asoslangan zaifliklar yotadi. Ijtimoiy muhandislik metodlarining klassik manipulyatsiyalardan sun’iy intellekt va deepfake texnologiyalarigacha bo‘lgan evolyutsion yo‘li ko‘rsatib berganidek, hujumchilar tizimni emas, balki tizim foydalanuvchisini nishonga olmoqda. Shuning uchun zamonaviy kiberhimoya strategiyalari faqat texnik vositalarga tayanib qolmasligi, balki inson omilini inobatga olgan holda, kiber-savodxonlikni oshirish va "Zero Trust" tamoyillarini joriy etish orqali kompleks yondashuvni talab etadi. Eng mukammal algoritmlar ham xato qilgan foydalanuvchi qarshisida ojiz qoladi.

FOYDALANILGAN ADABIYOTLAR

1. Abduhalikov, A. S. (2022). *Axborot xavfsizligi va kiber-psixologiya: Inson omili va ijtimoiy muhandislik xavflari tahlili.* Toshkent: "Fan va Texnologiya" nashriyoti.
2. Karimov, J. R. (2021). *Zamonaviy kiberxavfsizlik strategiyalari: Texnik va ijtimoiy zaifliklarni bartaraf etish usullari.* Samarkand: "O‘qituvchi" nashriyoti.
3. Mirzayev, B. T. (2023). *Raqamli dunyoda manipulyatsiya: Ijtimoiy muhandislik metodlarining evolyutsion rivojlanishi va kiber-tahdidlar.* Toshkent: "Akademika" nashriyoti.
4. Navrolov, S. M. (2020). *Axborot tizimlarida inson omili: Kiber-jinoyatchilikning psixologik va texnik jihatlari.* Andijon: "Universitet" nashriyoti.
5. Rahimov, O. K. (2019). *Kiberxavfsizlik asoslari: Axborotni himoya qilishda inson xatolari va ularning oqibatlari.* Buxoro: "Ilm" nashriyoti.
6. Toshpo‘latov, D. A. (2024). *Sun’iy intellekt davrida ijtimoiy muhandislik: Deepfake va yangi avlod kiber-hujumlar tahlili.* Toshkent: "Yangi asr" nashriyoti.