KIBERXAVFSIZLIK: SHAXSIY MA’LUMOTLARNI HIMOYA QILISH USULLARI

Xoshimova Durdona Sharofiddin qizi
Yuldasheva Elmira Xaitbayovna
Ohangaron shahar Politexnikumi

Annotatsiya: Ushbu maqolada shaxsiy ma'lumotlarni ruxsatsiz kirish va kiber tahdidlardan himoya qilishga qaratilgan turli kiberxavfsizlik usullari ko'rib chiqiladi. Ushbu maqola eng so'nggi xavfsizlik choralari, jumladan, shifrlash, ko‘p faktorli autentifikatsiya va sun'iy intellekt asosidagi xavfsizlik yechimlarini ko‘rib chiqadi. Shuningdek, maqolada zaif kiberxavfsizlik amaliyotlarining oqibatlari tahlil qilinadi va shaxsiy ma'lumotlarni himoya qilish bo‘yicha tavsiyalar beriladi.

Kalit so‘zlar: Kiberxavfsizlik, shaxsiy ma'lumotlarni himoya qilish, shifrlash, ko‘p faktorli autentifikatsiya, sun'iy intellekt, kiber tahdidlar, xavfsizlik choralari.

Raqamli davrda shaxsiy ma'lumotlar eng qimmatli aktivlardan biriga aylandi, shu sababli u kiberjinoyatchilarning asosiy nishoniga aylangan. Fishing, ransomware va shaxsiylikni o‘g‘irlash kabi kiber tahdidlarning ko‘payishi bilan shaxsiy ma'lumotlarni himoya qilish muhim masalaga aylandi. Ushbu maqolada shaxsiy ma'lumotlarni himoya qilishda qo‘llaniladigan asosiy usullar va ularning kiber xatarlarni kamaytirishdagi samaradorligi tahlil qilinadi.

Ushbu tadqiqot sifatli yondashuvdan foydalanib, mavjud kiberxavfsizlik texnikalarini tahlil qiladi va ularning samaradorligini baholaydi. Asosiy usullar quyidagilarni o‘z ichiga oladi:

- Shifrlash: Ma'lumotlarni faqat ruxsat etilgan foydalanuvchilar uchun mavjud bo‘lgan xavfsiz formatga aylantirish jarayoni.
- Ko‘p faktorli autentifikatsiya (MFA): Kirish huquqini olishdan oldin bir nechta tasdiqlash usullarini talab qiluvchi xavfsizlik chorasi.
- Sun'iy intellekt asosidagi xavfsizlik yechimlari: Noyob naqshlarni va mumkin bo‘lgan tahdidlarni real vaqt rejimida aniqlaydigan AI algoritmlari.
- Tarmoq xavfsizlik choralari: Ma'lumot uzatish xavfsizligini ta’minlash uchun firewall, kirishni aniqlash tizimlari (IDS) va VPN texnologiyalaridan foydalanish.
- Foydalanuvchilarni o‘qitish va xabardorlik: Foydalanuvchilarga xavfsiz onlayn amaliyotlarni o‘rgatish orqali ma'lumotlarning buzilishining oldini olish.

Raqamli platformalardan foydalanish ortib borayotgan bir paytda, shaxsiy ma'lumotlarni himoya qilish yanada muhim ahamiyat kasb etmoqda. Quyida ma'lumotlaringizni kiber tahdidlardan himoya qilishning asosiy usullari keltirilgan:

Kuchli va noyob parollardan foydalaning

- Katta-kichik harflar, raqamlar va maxsus belgilarni o‘z ichiga olgan murakkab parollar yarating.

- Bir xil paroldan bir nechta akkauntlar uchun foydalanmang.

- Parol menejeri yordamida parollarni xavfsiz saqlang va yaratish jarayonini avtomatlashtiring.

Ikki bosqichli autentifikatsiyani (2FA) yoqing

- Iloji boricha akkauntlaringiz uchun 2FA funksiyasini yoqing (SMS, email yoki autentifikatsiya ilovalari orqali).

- Bu parolingiz buzilgan taqdirda ham qo‘shimcha himoya qatlamini yaratadi.

Fishing hujumlariga e’tibor bering

- Noma’lum manbalardan kelgan shubhali havolalarni bosmang.

- Ma’lumot kiritishdan oldin jo‘natuvchini tekshiring.

- Imlo xatolari, shoshilinch so‘rovlar yoki tanish bo‘lmagan jo‘natuvchilar kabi belgilarni aniqlashga harakat qiling.

Qurilmalar va tarmoqlaringizni himoya qiling

- Kompyuteringizda antivirus va anti-malware dasturlaridan foydalaning.

- Operatsion tizim va ilovalarni doimiy ravishda yangilab boring.

- Begona kirishlarni oldini olish uchun firewall (xavfsizlik devori) o‘rnating.

Xavfsiz ulanishlardan foydalaning

- Jamoat Wi-Fi tarmoqlarida maxfiy operatsiyalarni bajarmang.

- Internet ulanishingizni shifrlash uchun VPN (Virtual Xususiy Tarmoq) dan foydalaning.

- Ma’lumot kiritishdan oldin saytning HTTPS bilan boshlanishini tekshiring.

Ijtimoiy tarmoqlarda ehtiyot bo‘ling

- Internetda ortiqcha shaxsiy ma’lumotlaringizni oshkor qilmang.

- Maxfiylik sozlamalarini o‘zgartirib, faqat tanish odamlarga ma’lumot ko‘rinishini ta’minlang.

- Noma’lum shaxslardan kelgan do‘stlik so‘rovlariga shoshilinch javob bermang.

Muhim ma’lumotlarni shifrlang

- Muhim hujjatlarni saqlash va jo‘natish uchun shifrlash vositalaridan foydalaning.

- Maxfiy ma’lumotlarni elektron pochta orqali yuborayotganda shifrlash texnologiyalaridan foydalaning.

Ma’lumotlaringizni muntazam zaxiralang

- Muhim ma’lumotlaringizni bir necha joyda saqlang (bulut xotirasi, tashqi xotira qurilmalari).

- Zaxiralangan ma’lumotlarni shifrlash orqali ruxsatsiz kirishlardan himoya qiling.

Moliyaviy operatsiyalarni kuzatib boring

- Bank hisoblaringizdagi harakatlarni muntazam tekshiring.
- G‘ayritabiiy operatsiyalarni oldindan bilish uchun xavfsizlik bildirishnomalarini yoqing.
- Onlayn xaridlar paytida xavfsiz to‘lov tizimlaridan foydalaning.

O‘z bilimlaringizni oshiring va yangiliklardan xabardor bo‘ling

- Eng so‘nggi kiber tahdidlardan xabardor bo‘lib boring.
- Kiberxavfsizlik bo‘yicha treninglar va seminarlar o‘tkazing yoki ularga qatnashing.
- Mutaxassislar tomonidan tavsiya etilgan eng yaxshi amaliyotlarga amal qiling.

Bu usullardan foydalanish shaxsiy ma’lumotlaringizni buzilish va o‘g‘irlikdan himoya qilishga yordam beradi. Kiberxavfsizlik doimiy jarayon bo‘lib, hushyorlik va ehtiyotkorlik muhim ahamiyatga ega.

Texnologik taraqqiyot shaxsiy ma'lumotlarni himoya qilish usullarini takomillashtirgan bo‘lsa-da, rivojlanayotgan kiber tahdidlar va xavfsizlik borasidagi xabardorlikning yetarli emasligi muammosi hanuzgacha mavjud. Kiberjinoyatchilar xavfsizlik choralari chetlab o‘tish uchun tobora murakkablashgan texnikalarni ishlab chiqmoqdalar, bu esa kiberxavfsizlik strategiyalarini doimiy ravishda yangilashni talab qiladi. Bundan tashqari, AI asosidagi xavfsizlik yechimlari atrofidagi maxfiylik masalalari shaxsiy ma'lumotlarni kuzatish va nazorat qilish bo‘yicha axloqiy muammolarni keltirib chiqaradi. Zamonaviy kiberxavfsizlik tizimlarida xavfsizlik va maxfiylik o‘rtasida muvozanatni saqlash asosiy muammo bo‘lib qolmoqda.

Xulosa

Shaxsiy ma'lumotlarni himoya qilish texnologik yechimlar bilan foydalanuvchilarning xabardorligini oshirishni o‘z ichiga olgan ko‘p qavatli yondashuvni talab qiladi. Asosiy tavsiyalar quyidagilarni o‘z ichiga oladi:

Muhim ma'lumotlar uchun mustahkam shifrlash va MFA protokollarini joriy etish.

Kiber tahdidlarni aniqlash va ularga javob berish uchun AI asosidagi xavfsizlik tizimlarini takomillashtirish.

Ommaviy xabardorlik va kiberxavfsizlik bo‘yicha trening dasturlarini kuchaytirish.

Dasturlar va xavfsizlik yangilanishlarini muntazam ravishda o‘rnatish orqali zaifliklarni bartaraf etish.

Hukumatlar va tartibga soluvchi organlar tomonidan qat'iy kiberxavfsizlik qoidalarini ishlab chiqish va amalga oshirish.

Ushbu choralarni amalga oshirish orqali jismoniy shaxslar va tashkilotlar shaxsiy ma'lumotlarning buzilish xavfini sezilarli darajada kamaytirishlari va umumiy kiberxavfsizlik barqarorligini mustahkamlashlari mumkin.

Adabiyotlar.

1. VV Byts', RM Zulunov. Specification of matrix algebra problems by reduction. Journal of Mathematical Sciences. T. 71, 2719–2726 (1994).
2. Web Server and its Types of Attacks [Electronic resource] // URL: https://www.greycampus.com/opencampus/ethical hacking/web-server-and-its-types-of-attacks.
3. The NIST Definition of Cloud Computing [Electronic resource] // URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecia lpublication800-145.pdf.
4. Advanced persistent threat [Electronic resource] // URL: https://en.wikipedia.org/wiki/Advanced_persistent_thr eat.
5. Stallings W. Cryptography and Network Security: Principles and Practice, 7th Edition / W. Stallings. - London: Pearson plc, Cop. 2017. - 766 p.
6. Р. Зулунов, А.Горовик. Внедрение технологий искусственного интеллекта, нравственные и правовые нормы. Conference on Digital Innovation: "Modern Problems and Solutions", 2023.
7. R.Zulunov. Pythonda neyron tarmoqni qurish va bashorat qilish. Al-Farg'oniy avlodlari, 2023, 1/4, c. 22-26.
8. R Zulunov, O Otaqulov. Ограничения обучения языку программирования JAVA в образовательных системах. Потомки Аль-Фаргани, 2023, т.1/2, с. 37-40