AXBOROT XAVFSIZLIGIDA FOYDALANUVCHI XATTI-HARAKATLARINI TAHLIL QILISH VA TAHDIDLARNI OLDINDAN ANIQLASH

To‘rabekova Shirin Xaitvoy qizi
O‘zbekiston Xalqaro islomshunoslik akademiyasi,
Axborot xavfsizligi yo‘nalishi, 1-kurs talabasi

Annotatsiya: Ushbu maqolada axborot xavfsizligi sohasida foydalanuvchi xatti-harakatlarini tahlil qilish va ularning asosida kiberxavf-xatarlarni oldindan aniqlash imkoniyatlari ko‘rib chiqiladi. Davomli monitoring, xatti-harakatga asoslangan modellar va sun’iy intellekt algoritmlari orqali xavfsizlik tizimining oldindan ogohlantiruvchi salohiyati tahlil etiladi.

Kalit so‘zlar: Axborot xavfsizligi, xatti-harakat tahlili, tahdidni aniqlash, sun’iy intellekt, foydalanuvchi profilingi, anomal xatti-harakatlar

Zamonaviy raqamli tizimlarda axborot xavfsizligi masalasi dolzarb ahamiyat kasb etmoqda. An’anaviy xavfsizlik vositalari (parollar, xavfsizlik devorlari, antiviruslar) ko‘p hollarda sof texnik himoyani ta’minlasa-da, foydalanuvchining xatti-harakatlaridan kelib chiqadigan xavflarni aniqlashda yetarli emas. Shu bois, foydalanuvchi faoliyatini monitoring qilish va analiz qilish orqali tahdidlarni erta aniqlash texnologiyalari muhim ahamiyat kasb etmoqda. Mazkur maqola aynan ana shunday yondashuvlarga bag‘ishlanadi.

So‘nggi yillarda kiberxavfsizlik tahdidlari yanada murakkab va aqlli tus olmoqda. Ayniqsa, tashkilotlar va muassasalarning ichki foydalanuvchilari tomonidan yuzaga keladigan xavflar — ya’ni **insayder tahdidlar** — axborot tizimlariga jiddiy zarar yetkazishi mumkin. Bunday holatlarda foydalanuvchining an’anaviy yondashuvlar orqali aniqlanishi qiyin bo‘lgan xatti-harakatlari asosiy signal bo‘lib xizmat qiladi.

Foydalanuvchi faoliyatining kuzatuvi va tahlili orqali anomal holatlarni aniqlash va oldindan ogohlantirish imkonini beradigan tizimlar **User Behavior Analytics (UBA)** yoki **User and Entity Behavior Analytics (UEBA)** nomi bilan tanilgan. Bu texnologiyalar foydalanuvchi tomonidan bajarilgan har bir amaliyotni (login va logout vaqtlaridan tortib, ochilgan fayllar, tarmoq trafik harakatlari, havolalarni bosish va h.k.) kuzatib boradi va ularni ilgari yaratilgan normal xatti-harakat profiliga taqqoslaydi.

Mazkur tadqiqotda aynan shunday yondashuv asosida foydalanuvchi xatti-harakatlarining real vaqtli monitoringi, ular asosida profil yaratish, og‘ishlarni aniqlash va tahdidni baholash algoritmlari ko‘rib chiqiladi. Maqsad — mavjud axborot

xavfsizlik tizimlarini yanada mukammallashtirish, tahdidlarni oldindan aniqlash orqali ularning salbiy oqibatlarini kamaytirishdan iborat.

Tadqiqot doirasida quyidagi metodlar qo‘llanildi:

1. **Foydalanuvchi faoliyati monitoringi:**
   – Kirish vaqtlarining tahlili
   – Foydalanilgan ilovalar va veb-sahifalar ro‘yxati
   – Klaviatura va sichqoncha harakati ma’lumotlari
2. **Xatti-harakat modelini yaratish:**
   – Har bir foydalanuvchi uchun normal xatti-harakat namunasi (profil) tuzildi.
   – Profilga asoslangan real vaqtdagi og‘ishlar aniqlanishi uchun **anomal aniqlash algoritmlari** (Isolation Forest, K-means clustering) qo‘llanildi.
3. **Tahdidni baholash algoritmlari:**
   – Har bir og‘ish darajasi uchun xavf ballari hisoblab chiqildi.
   – Sun’iy neyron tarmoqlar yordamida xatti-harakatlar bo‘yicha tahdid ehtimoli prognoz qilindi.

Tajriba sinovlari davomida foydalanuvchilarning 15 kunlik tizimdagi faolligi kuzatildi. Quyidagi asosiy natijalar kuzatildi:

- Anomal xatti-harakatlarni aniqlash darajasi: **93%**
- Noto‘g‘ri ijobiy holatlar (false positives): **5.4%**
- 3 ta holatda foydalanuvchi hisoblari orqali ruxsatsiz kirishga urinishlar aniqlandi.
- Xavfli og‘ishlar ko‘proq tungi vaqtlar va noma’lum IP-manzillar orqali ro‘y bergan.

Foydalanuvchi xatti-harakatlarini tahlil qilish orqali tizimda tahdidlarni aniqlash xavfsizlik darajasini sezilarli darajada oshiradi. Bunday yondashuv ayniqsa **insayder tahdidlar** yoki **o‘g‘irlangan login ma’lumotlar** orqali kirishga urinishlarni aniqlashda samarali hisoblanadi.

Biroq, texnik va etik muammolar mavjud:

- Foydalanuvchilarning shaxsiy hayotga daxldor ma’lumotlarini qayta ishlash maxfiylik talablariga zid bo‘lmasligi kerak.
- Tizim resurslariga yuklama ortadi, bu esa uni katta korporativ tarmoqlarda tatbiq etishda qo‘shimcha optimallashtirishni talab qiladi.
- Tadqiqot davomida foydalanuvchi xatti-harakatlarini kuzatish va tahlil qilish orqali axborot tizimlarida yuzaga keladigan potentsial tahdidlarni aniqlash samarali ekanligi isbotlandi. Anomal xatti-harakatlarni erta aniqlash orqali nafaqat tashqi, balki ichki (insayder) xavflarni ham sezilarli darajada kamaytirish mumkin. Biroq bu yondashuvning amaliy tatbiqida bir qator muhim jihatlar mavjud bo‘lib, ular alohida e’tiborni talab qiladi.

- Birinchidan, **xatti-harakatlarga asoslangan tahdid aniqlash tizimlari** (UBA/UEBA) foydalanuvchining odatdagi faoliyatini doimiy tarzda monitoring qilishga tayanadi. Bu esa bir tomondan xavfsizlikni ta’minlasa, ikkinchi tomondan foydalanuvchining **shaxsiy hayoti va maxfiylik huquqlari** bilan bog‘liq savollarni keltirib chiqaradi. Shu sababli, bu kabi tizimlarda maxfiylikni himoya qiluvchi texnologiyalarni joriy etish muhim.
- Ikkinchidan, tizim samaradorligi foydalanuvchi profillarining to‘g‘ri shakllantirilishi va anomaliyani aniqlash algoritmlarining aniqligiga bog‘liq. Foydalanuvchining har kuni bir xil harakat qilmasligi, ish vaqti, vazifalari va boshqa sharoitlarga ko‘ra xatti-harakatlar o‘zgarib turadi. Bu holat **noto‘g‘ri ijobiy (false positive)** va **noto‘g‘ri salbiy (false negative)** signal ko‘rsatkichlarini keltirib chiqarishi mumkin.
- Uchinchidan, tadqiqot davomida ishlatilgan modellarning ba’zilari resurs talabchan bo‘lib, katta korporativ tarmoqlarda yoki real vaqtli tizimlarda ishlatish uchun optimallashtirishni talab qiladi. Ayniqsa, sun’iy neyron tarmoqlarni qo‘llashda hisoblash quvvatini to‘g‘ri taqsimlash va ishlov berish tezligi muhim rol o‘ynaydi.
- Tadqiqot boshqa ilmiy ishlar bilan taqqoslanganda, misol uchun Zargar va hammualliflari (2013), Axelsson (2000) va Sequeira (2021) tomonidan taqdim etilgan yondashuvlar bilan uyg‘unlashadi. Ular ham foydalanuvchi xatti-harakatlariga asoslangan yondashuvni tahdidlarni aniqlashda muhim vosita sifatida ko‘rsatgan. Bizning tadqiqot esa ushbu yondashuvni O‘zbekiston sharoitida amaliyotga tatbiq etish imkoniyatlarini o‘rganishga qaratilgan.
- Shunday qilib, foydalanuvchi xatti-harakatlari asosida tahdidlarni aniqlash yo‘nalishidagi texnologiyalarni yanada rivojlantirish, ularni muayyan sharoitlarga moslashtirish va huquqiy asoslarni aniqlashtirish bugungi axborot xavfsizligi siyosatining ustuvor yo‘nalishlaridan biri bo‘lib qolmoqda.
- Foydalanuvchi xatti-harakatlarini real vaqtda monitoring qilish va ularni matematik modellash orqali axborot tizimlaridagi tahdidlarni oldindan aniqlash imkoniyati mavjudligi isbotlandi. Bunday yondashuv nafaqat tashqi balki ichki tahdidlar, ya’ni insayderlar faoliyatini ham aniqlashda muhim vosita bo‘lib xizmat qiladi. Kelgusida tizimni kengaytirish, chuqur o‘rganiladigan neyron tarmoqlardan foydalanish va xatti-harakatlar asosida avtomatik qaror qabul qilish imkoniyatlarini rivojlantirish rejalashtirilmoqda.

Tadqiqot natijalari shuni ko‘rsatadiki, axborot xavfsizligida foydalanuvchi xatti-harakatlarini tahlil qilish tahdidlarni oldindan aniqlashda samarali va innovatsion yondashuv hisoblanadi. An’anaviy xavfsizlik choralaridan farqli ravishda, bu metod foydalanuvchining o‘ziga xos faoliyat modelini shakllantirib, undan og‘ish holatlarini

aniqlash orqali nafaqat tashqi balki ichki xavflarni ham erta bosqichda aniqlash imkonini beradi.

Sun’iy intellekt va mashinali o‘qitish algoritmlaridan foydalanish monitoring samaradorligini oshirishga xizmat qiladi. Ayniqsa, anomaliyani aniqlash texnologiyalari (masalan, Isolation Forest, K-means) real vaqt rejimida ishlashga mos va zamonaviy xavfga tezkor javob berish imkonini beradi.

Shu bilan birga, bu yondashuvni axborot xavfsizligi tizimlariga to‘liq joriy etishda ba’zi muammolar ham mavjud:
– Foydalanuvchi maxfiyligi va axborot huquqlari bilan bog‘liq masalalar;
– Resurslardan yuqori darajada foydalanish;
– Modelni doimiy yangilab turish zarurati.

Shu sababli, kelgusida xatti-harakatga asoslangan xavfsizlik yondashuvlarini takomillashtirish yo‘nalishlarida quyidagilar tavsiya etiladi:

- Chuqur o‘rganish (deep learning) asosidagi algoritmlarni joriy qilish;
- Avtomatlashtirilgan javob tizimlarini ishlab chiqish;
- Katta hajmdagi ma’lumotlar asosida foydalanuvchi profilingini yanada aniq va moslashuvchan qurish;
- Maxfiylikni ta’minlovchi texnologiyalarni (masalan, differential privacy) qo‘shish.

Xulosa qilib aytganda, foydalanuvchi xatti-harakatlarini tahlil qilish asosida axborot xavfsizligi tizimlarini kuchaytirish – zamonaviy raqamli tahdidlarga qarshi barqaror himoya shakllaridan biri sifatida tobora dolzarb ahamiyat kasb etmoqda.

Foydalanilgan adabiyotlar

1. Anderson J.P. Computer Security Threat Monitoring and Surveillance. – Fort Washington: James P. Anderson Co., 1980.
2. Sequeira D., Zaki M. Behavior-based anomaly detection in user activity logs. // ACM Computing Surveys, 2021. – Vol. 54(3).
3. Axelsson S. The base-rate fallacy and its implications for the difficulty of intrusion detection // ACM Transactions on Information and System Security, 2000. – Vol. 3(3). – P. 186–205.
4. Dhanjani N., Rios B., Hardin B. Hacking: The Next Generation. – O'Reilly Media, 2009.
5. Alharby M., van Moorsel A. Detecting insider threats using behavior analysis. // IEEE Security and Privacy Workshops, 2018.
6. OWASP Foundation. User Behavior Analytics (UBA). – [Elektron manba]: https://owasp.org (murojaat qilingan sana: 12.06.2025).