BANK ISHIDA KIBER XAVFSIZLIK MASALASI VA MIJOZLAR MA'LUMOTLARINI HIMOYA QILISH

Akramov Xurshidbek Bahrom og'li
Andijon iqtisodiyot va qurilish instituti Iqtisodiyot fakulteti 3-kurs talabasi
https://doi.org/10.5281/zenodo.11090660

Annotatsiya: Ushbu maqola bank sohasida kiberxavfsizlik choralarining muhim ahamiyatini va moliya institutlariga tegishli bo'lgan keng va nozik ma'lumotlarni himoya qilish zarurligini takidlaydi. Kiber tahdidlar yanada murakkab borar ekan, ma'lumotlarning buzilishi, o'g'irlanishi va moliyaviy firibgarliklarning potensial ortib bormoqda, bu esa mustahkam va faol kiberxavfsizlik strategiyalarini talab qiladi.
Kalit so'zlar: Kiberxavfsizlik, bank ishi, mijozlar ma'lumotlari, raqamli asr, ma'lumotlarni himoya qilish, kiber tahdidlar, firibgarlikning oldini olish, tartibga rioya qilish.

Kiberxavfsizlik bugungi o'zaro bog'liq dunyoda, xususan, moliyaviy landshaftda muhim rol o'ynaydi. Moliyaviy operatsiyalar, ma'lumotlarni saqlash va aloqa uchun raqamli platformalarga bo'lgan ishonch ortib borayotganligi sababli, kiberjinoyatchilar tomonidan yuzaga kelishi mumkin bo'lgan tahdidlar yanada kengroq va murakkablashdi. Moliyaviy sektorda muvaffaqiyatli kiberhujumning oqibatlari halokatli bo'lishi mumkin, bu moliyaviy yo'qotishlarga, obro'siga putur etkazishga va mijozlar ishonchini buzishga olib keladi. Shunday qilib, moliyaviy institutlar o'z aktivlari va mijozlari manfaatlarini himoya qilish uchun kuchli kiberxavfsizlik choralariga sarmoya kiritishlari shart. Alohida moliyaviy institutlarni himoya qilishdan tashqari, moliyaviy landshaftdagi kiberxavfsizlik global iqtisodiyot barqarorligini saqlash uchun muhim ahamiyatga ega. Yirik moliya institutiga kiberhujum moliyaviy bozorlarni buzishi, investorlarning ishonchiga putur etkazishi va keng qamrovli oqibatlarga olib kelishi mumkin bo'lgan tizimli xavflarni keltirib chiqarishi mumkin. Ko'proq jismoniy shaxslar va korxonalar o'zlarining moliyaviy faoliyati uchun raqamli tranzaktsiyalarga tayanar ekan, ushbu platformalarni kiber tahdidlardan himoya qilish zarurati birinchi o'ringa chiqdi.

Bank sohasiga keladigan bo'lsak, Kiberxavfsizlik bank tizimiga ishonch va ishonchni saqlab qolish uchun zarurdir. Mijozlar onlayn tranzaktsiyalarni amalga oshirishda, hisob balanslarini tekshirishda yoki mobil bank ilovalaridan foydalanishda shaxsiy va moliyaviy ma'lumotlarining xavfsiz bo'lishini kutishadi. Kiberxavfsizlikning buzilishi jiddiy oqibatlarga olib kelishi mumkin, jumladan, moliyaviy yo'qotish, shaxsni o'g'irlash va bank obro'siga putur etkazish. Banklarga kiberxavfsizlik nima uchun kerak? "Kiberxavfsizlik" deb ataladigan texnologiyalar, protokollar va usullarning joylashuvi hujumlar, shikastlanishlar, zararli dasturlar, viruslar, xakerlik va mijozlar turli ma'lumotlariga ruhsatsiz kirishdan himoya qilish uchun mo'ljallangan.

Banklarda kiberxavfsizlik masalasiga respublikamizda jiddiy e'tiborlar qaratila boshlandi. Ya'ni "Banklar va bank faoliyati to'g'risida"gi qonunning 54-moddasiga muvofiq bank axborot va kiberxavfsizlikni ta'minlash bo'yicha qonunchilik talablarini buzganligi qo'pol qoidabuzarliklar qatoriga kiritilmoqda.

Ushbu qonunga ko'ra, qoida buzarliklar amalga oshirilganda Markaziy bank tijorat banklariga sanksiyalar qo'llaydi:

- Banklar va bank faoliyati tog’risidagi qonunchilikni buzgan holda amalga oshirilgan moliyaviy operatsiyalardan olingan daromadlarning miqdorini aniqlash imkoni bo’lsa, bankdan ushbu daromadlarning ikki baravari miqdoridan yoki bank tomonidan o’tgan moliya yili davomida olingan sof foydaning besh foizi yoki bank jami kapitalining bir foizi miqdoridan ortiq bo’lmagan miqdorda jarima
- Litsenziyani chiqarib olishga

Bank kuzatuv kengashining, boshqaruvi azosidan jarima qo’llanilayotgan oydan avvalgi yil ichida olingan mukofotning yuz foizidan ortiq bo’lmagan miqdorda jarima undirishga va boshqalar. So'ngi bir necha yil ichida kiberjinoyatlar tez-tez ko'payib bordi, ular moliyaviy sektor uchun eng muhim xavflardan biri deb o'ylashadi. Xakerlar o'zlarining texnologiyalari va tajribalarini yaxshiladilar, bu esa har qanday bank sektoriga hujumni doimiy ravishda oldini olishni qiyinlashtirdi. Quyida banklarning kiberxavfsizligi uchun ba'zi xavflar keltirilgan: 1) fishing hujumlari- ular moliya instituti tarmog'iga kirish va APT kabi jiddiy hujumni amalga oshirish uchun ishlatilishi mumkin, bu esa ushbu tashkilotlarga halokatli ta'sir ko'rsatishi mumkin, 2) troyanlar- ushbu turdagi kompyuter dasturida kompyuterga tashqaridan kirish imkonini beruvchi orqa eshik mavjud. 3) to’lov dasturi- To'lov dasturi deb nomlanuvchi kiber tahdid muhim ma'lumotlarni shifrlaydi va egalari yuqori narx yoki to'lovni to'lamaguncha ularga kirishiga to'sqinlik qiladi. Ma'lumotlaringiz va tizimlaringizni himoya qilish uchun kiberxavfsizlik vositalari va yondashuvlarini tanlash juda muhimdir. Mana bir nechta muhim kiberxavfsizlik vositalari:

1. Tarmoq Xavfsizligi Nazorati. Tarmoq monitoringi xavfli yoki intruziv xatti-harakatlar belgilari uchun tarmoqni doimiy ravishda skanerlash deb nomlanadi. U ko'pincha xavfsizlik devorlari, antivirus dasturlari va identifikatorlar (kirishni aniqlash tizimi) kabi boshqa xavfsizlik echimlari bilan qo'llaniladi. Dastur tarmoq xavfsizligini qo'lda yoki avtomatik ravishda kuzatishga imkon beradi.

2. Dastur Xavfsizligi. Ilova xavfsizligi biznes operatsiyalari uchun zarur bo'lgan dasturlarni himoya qiladi. U ro'yxatga olish va kod imzolashga ruxsat beruvchi dastur kabi xususiyatlarga ega va xavfsizlik siyosatingizni fayl almashish ruxsatnomalari va ko'p faktorli autentifikatsiya bilan sinxronlashtirishga yordam beradi. Kiberxavfsizlikda sun'iy intellektdan foydalanish muqarrar ravishda dasturiy ta'minot xavfsizligini yaxshilaydi.

3. Xatarlarni Boshqarish. Moliyaviy kiberxavfsizlik xatarlarni boshqarish, ma'lumotlar yaxlitligi, xavfsizlik to'g'risida xabardorlik bo'yicha trening va xavflarni tahlil qilishni o'z ichiga oladi. Xatarlarni boshqarishning muhim elementlariga xavflarni baholash va ushbu xavflardan zararni oldini olish kiradi. Ma'lumotlar xavfsizligi, shuningdek, nozik ma'lumotlarning xavfsizligini hal qiladi.

4. Muhim Tizimlarni Himoya Qilish. Keng tarmoq ulanishlari katta tizimlarga hujumlardan qochishga yordam beradi. Bu o'z qurilmalarini himoya qilish uchun kiberxavfsizlik choralarini ko'rishda foydalanuvchilar uchun sanoat tomonidan belgilangan qattiq xavfsizlik standartlarini qo'llab-quvvatlaydi. U barcha dasturlarni doimiy ravishda kuzatib boradi va foydalanuvchilar, serverlar va tarmoqdagi xavfsizlik tekshiruvlarini amalga oshiradi.

Xulosa qilganda, kiberxavfsizlik raqamli asrda bank faoliyatining asosiy jihati bo‘lib, mijozlar ma’lumotlari himoyasini ta’minlaydi va bank tizimiga ishonch va ishonchni saqlab qoladi. Kiberxavfsizlik bo'yicha qat'iy choralarni amalga oshirish, tartibga solish talablariga rioya qilish va doimiy innovatsiyalar va moslashishga sarmoya kiritish orqali banklar

kibertahdidlar bilan bog'liq xavflarni samarali tarzda yumshata oladi va mijozlarga xavfsiz va ishonchli bank muhitini taqdim etadi.

References:

1. S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov. Kiberxavfsizlik asoslari: O'quv qo'llanma. – T.: «Aloqachi», 2020, 221 bet.
2. Cyber Security Policy Guidebook
3. "Banklar va bank faoliyati to'g'risida"gi qonun, 05.11.2019 yildagi O'RQ-580-son
4. www.knowledgehut.com