SCIENCE BOX

Journal of Advanced Research and Stability
Volume: 02 Issue: 12 | Dec - 2022 *ISSN: 2181-2608*
www.sciencebox.uz

BANKLARDA KIBER XAVFSIZLIK MASALASIDAGI MUAMMOLAR VA ULARNI YECHISH

Narqabilov Aziz Raxmatillayevich
Toshkent davlat yuridik universiteti magistratura bosqichi talabasi, narkabilov.aziz@mail.ru

Annotatsiya*: Oxirgi asrda aynan bank sektori kiber jinoyatlar tufayli eng ko'p hujum qilingan tarmoqlar reytingida birinchi o'rinni egallab kelmoqda. Kompyuter hali paydo bo'lmaganida, pul banklardan jismoniy shaklda faol ravishda o'g'irlangan. Kompyuterlar, ayniqsa Internet keng qo'llanilganda, o'sha paytdan boshlab raqamli texnologiyalarni suiiste'mol qilish boshlandi. Ba'zi zararli dasturlardan foydalangan holda kompyuter orqali siz bir daqiqada bir nechta kompyuterlarni buzishingiz mumkin. Xakerlar bunday ish uchun maxsus o'qitilgan.*

Bank sohasida ishlaydigan odamlar endi moliyaviy operatsiyalarni boshlash uchun texnologiyaga tayanmoqdalar va shuning uchun hamma narsa izsiz o'g'irlanishi mumkin. Ushbu maqolada bank sektorining kiber xavfsizlik ahamiyati e'tirof etiladi.

Kalit so'zlar: *bank sektori, raqamli texnologiyalar, zararli dasturlar, moliyaviy operatsiyalar, izsiz o'g'irlanish, kiberxavfsizlik.*

Bibliografiya:

1. Information Security and Cyber Law by Vishal Baldaniya
2. The importance of cyber security in banking by Prem Khatri
3. Digital Banking and Cyber Security by Dr Sarika R Lohana
4. https://www.bankbusiness.us/the-importance-of-cybersecurity-in-banking/

Reja:

1) Kiberhujumlar turlari.
2) Qanday qilib bankda kiber xavfsizlikni rivojlantirsak bo'ladi ?
3) Bankda kiberxavfsizlik uchun javob beradigan insonlar va himoya tizimlari
4) Kiberxavfsizlik muhim bo'lgan boshqa sohalar.

Kiberhujumlar turlari:

1. Mobil ilovalar orqali.

Mijozlar ishlatadigan dasturlarning xavfsizlik tizimini busish mumkun. Ko'pgina foydalanuvchilar o'zlarining mobil telefonlarini himoya qilishni bilishmaydi yoki ushbu uchinchi tomon dasturlari tomonidan osonlikcha ushlanib qolishadi. Ushbu qurilmalarda xavfsizlik parametrlari pastligicha qolayotganligi uchun, kiberjinoyatchilik ehtimoli oshadi. Qaysi mobil ilova haqiqiy ekanligini va uni yuklab olish va unga kirishdan oldin unga ishonishingiz mumkinligini bilishingiz kerak.

2. Uchinchi shaxsning ishtiroki tufayli yuzaga keladigan ma'lumotlarning buzilishi

Kiberjinoyatchilar har doim tizimlarni buzish va maqsadlariga erishishning yangi usullarini

izlashadi. Tranzaktsiyalarning silliqligini ta'minlaydigan yangi bank tizimlari va onlayn texnologiyalar boshqa dunyoqarashga yo'l ochdi. Endi mijozlar ham, banklar ham onlayn tizimlarga bog'liq va bu xakerlarga ushbu urinishlarni muvaffaqiyatli amalga oshirish uchun hech qanday standart protokolga ega bo'lmagan holda uchinchi tomon tizimlari bilan bog'langan ushbu tizimlardan foydalanishga imkon berdi. Agar ushbu tizimlar tegishli kiberxavfsizlik choralari bilan himoyalanmagan bo'lsa, unda kiberjinoyatchilik doimiy ravishda o'sib boradi.

Qanday qilib bankda kiber xavfsizlikni rivojlantirsak bo'ladi ?

1. Xodimlarni xavfsizlik buzilishi to'g'risida xabardor qilish

Xakerlar moliyaviy tizimlarni buzishi mumkinligini bilganimiz sababli, ular moliyaviy operatsiyalar uchun ishlatiladigan eng past himoyali tarmoqlarni to'liq egallab olishlari mumkin va moliya tizimida ishlaydigan xodimlar bilimi kamlik qiladi yoki bulardan bexabar qolishadi.

Birinchi va asosiy ish bu kiberxavfsizlikdan himoya qilishning ishonchli mexanizmini ta'minlash va xodimlarni tashkilot himoya tizimini buzmasliklari uchun nimalarga va shubxali savollarga e'tiborli bo'lishlarini o'rgatish kerak.

Shu sababli, bir bir kiber jinoyatlar va xabardorlikni oshirish bo'yicha uchrashuvlar va treninglar tashkil etish kerak, bu tashkilot tarmog'ining hech qanday uzilishlarsiz yaxshi ishlashini ta'minlash uchun kerakli masaladir.

Bundan tashqari, agar ular tranzaktsiyalarda biron bir shubhali narsa sezsalar, bular, pul ko'p aylantirish foydalanuvchilar tomonidan yoki boshqa shubhali ishlar, darhol kiberxavfsizlik xizmatiga xabar berishsin, shunda potentsial zararni oldini olish uchun qarshi choralar tezda qabul qilinadi.

2. Dasturiy ta'minot monitoringi va davriy auditni muntazam ravishda olib borish

Agar hech bo'lmaganda bir marta beetibor bo'linsa, jiddiy xavfsizlik muammolari bo'lishi mumkin va hamma narsa xakerning qo'llari bilan o'g'irlanishi mumkin.

O'zingizning sektoringizni, ayniqsa bank sektorini himoya qilishning yana bir usuli bor, shunda mijozlarning mablag'lari yoki boshqa narsalar buzilmaydi. Bu monitoring orqali sodir bo'lishi mumkin. Agar siz biron bir firibgarlikni sezmasangiz yoki tizimingiz yaxshi deb hisoblasangiz ham, yuzaga kelishi mumkin bo'lgan muammolarni topishingiz yoki har qanday noto'g'ri ishlarni tekshirishingiz va aniqlanishingiz kerak. Shuningdek, siz ushbu tizimni tartibga solishga yordam berish uchun bankingizda xavfsizlik auditi guruhini tayinlashingiz mumkin. Har kuni sizning tarmog'ingiz to'g'ri tekshirilishi va to'g'ri sozlanishi kerak.

3. Ishonchli sotuvchilardan dasturiy yechimlarni sotib olish.

Haqiqiy va ishonchli xavfsizlik yechimini tanlang. Agar siz uni barcha vositalar bilan tekshirmasangiz, ayanchli oqibatlarga olib kelishi mumkin bo'lgan xavfsizlik yechimiga ega bo'lishingiz mumkin. Avval siz uning qanchalik ishonchli ekanligini aniqlab olishingiz va keyin kiberxavfsizlikni avtomatik ravishda ta'minlash jarayonini boshlashingiz kerak. Yana bir talab bitta dasturiy taminotchidan ikkinchisiga doimiy ravishda o'tmaslik bo'ladi. Agar bitta tizim haqiqiy ekanligini aniqlasangiz, unda qoling va almashtirmang. Bu sizning tizimingizda har qanday zararli dasturni o'rnatish ehtimolini kamaytib yuboradi.

Yaxshi xavfsizlik dasturlari shundan iboratki, u hamma narsani himoya qiladi va shubhali ko'rinadigan narsalarni o'z-o'zidan o'tkazib yubormaydi. Ushbu turdagi himoya ayroportda screening kabi kuzatilgandek, har bir sektorda o'rnatilishi yaxshi natija beradi.

Bankda kiberxavfsizlik uchun javob beradigan insonlar va ularning himoya tizimlari

Axborot xavfsizligi bo'yicha bosh menejer

Axborot xavfsizligi bo'yicha bosh mutaxasis - bu bank muassasasining xavfsizligi uchun mas'ul bo'lgan yoki har qanday kibermakonda ma'lumot beradigan xodim.

Bu mutaxasisning asosiy ishi. Bu bankka ularning tizimi bilan bog'liq har qanday muammolarni aniqlashga yordam beradi. Mutaxasis har doim har bir operatsiya yoki vipiska to'g'risida yozuvlarni yuboradi, agar biron bir shubxani sezsa.

Davlat tomonidan taqdim etilgan bank himoya tizmlari mavjud. Bular FFIEC, Amerika hukumat idorasi, MAS, Singapur hukumat idorasi va boshqalar.

Kiberxavfsizlik muhim bo’lgan boshqa sohalar.

Biznes sohasi: har bir korxona o’z ishlab chiqarish, sotish va boshqa sirlari bo’ladi, bularning qo’riqlanish darajasi yaxshi bo’lishi kerak. Qo’shimcha qilib, bugungi kunda korxonalar o'z mijozlari va xodimlari to'g'risida maxfiy ma'lumotlarni saqlaydilar. Ushbu ma'lumotlar juda shaxsiydir va bu ma'lumotlarning tarqalishi biznes uchun pul yo'qotishlariga olib kelishi mumkin.

Mudofaa sektori: mudofaa sektori ham kuchli kiber mudofaa mexanizmiga muhtoj! Mudofaa sektori butun mamlakat xavfsizligi uchun javobgardir va shuning uchun ular xakerlardan uzoq turishlari juda muhimdir.

Tepada sanab o’tilgan faktlar va misollarni inobatga olib Kiberxavfsizlikni joriy qilish va rivojlantirish to’g’ri qaror bo’ladi.