“JOURNAL OF SCIENCE-INNOVATIVE RESEARCH IN UZBEKISTAN” JURNALI
VOLUME 2, ISSUE 1, 2024. JANUARY
ResearchBib Impact Factor: 8.654/2023 ISSN 2992-8869

AXBOROT KOMMUNIKATSIYA TIZIMLARIDA RUXSATSIZ FOYDALANISHLARNI ROLLI METODI ASOSIDA TAKOMILLASHTIRISH USULLARINI ISHLAB CHIQISH

Ilmiy rahbar: i.f.d., PhD **F.T.Jumayev**
Kompyuter tizimlari va ularning dasturiy ta’minoti
yo’nalishi magistranti **Jumayev Ulug‘bek Ulash o‘g‘li**

Annotatsiya: Bugungi raqamli asrda kiberhujumlar turli sohalarga, jumladan, hukumat, sog'liqni saqlash, moliya va energetika sohalariga qaratilgan yanada murakkablashdi. Hisob-kitoblarga ko‘ra, 2025-yilga borib kiberjinoyatlar jahon iqtisodiyotiga har yili 10,5 trillion dollar zarar keltiradi. Ushbu tahdidlardan samarali himoya qilish uchun tashkilotlar kiberxavfsizlik choralarini kuchaytirishlari va muhim aloqa tarmoqlarini himoya qilishga ustuvor ahamiyat berishlari kerak. Ushbu maqolada biz ruxsatsiz bosqinlardan himoya qilishning ahamiyatini o'rganamiz va muhim aloqa tarmoqlarini himoya qilishning samarali strategiyalarini muhokama qilamiz.

Kalit so’zlar: kiberxavfsizlik, autentifikatsiya, Shifrlash, Intrusionlarni aniqlash, Sun'iy intellekt (AI) va Machine Learning (ML), Zero Trust Architecture, Mustahkam xavfsizlik devori, Rolli metodi.

Muhim aloqa tarmoqlari ko'pincha maxfiy ma'lumotlarni o'z ichiga oladi, agar buzilgan bo'lsa, jiddiy oqibatlarga olib kelishi mumkin. Kuchli xavfsizlik choralarini qo'llash ma'lumotlarni ruxsatsiz kirishdan himoya qiladi, maxfiylik va maxfiylikni ta'minlaydi. Muvaffaqiyatli hujumlar aloqa tarmoqlarini buzishi mumkin, bu esa sezilarli uzilishlarga olib keladi va kundalik operatsiyalarga to'sqinlik qiladi. Tegishli xavfsizlik choralarini qo'llash uzluksiz aloqani ta'minlab, xizmat ko'rsatishda uzilishlar xavfini kamaytiradi.

Ruxsatsiz bosqinlardan himoya qilish texnik va operatsion choralarni o'z ichiga olgan ko'p qatlamli yondashuvni talab qiladi. Quyida ko'rib chiqilishi kerak bo'lgan ba'zi strategiyalar mavjud:

1. Kuchli autentifikatsiya mexanizmlarini amalga oshirish. Ikki faktorli autentifikatsiya (2FA) yoki biometrika kabi samarali autentifikatsiya mexanizmlari aloqa tarmoqlariga qo'shimcha xavfsizlik darajasini qo'shadi. Bir nechta hisobga

olish ma'lumotlari yoki noyob biologik xususiyatlarni talab qilish orqali ruxsatsiz kirish sezilarli darajada qiyinlashadi.

2. Tizimlarni muntazam yangilash va tuzatish. Dasturiy ta'minot va tizimlarni yangilab turish paydo bo'ladigan tahdidlardan himoyalanishda juda muhimdir. Muntazam yangilanishlar va yamoqlar zaifliklarni bartaraf etishga va muhim aloqa tarmoqlari xavfsizligini mustahkamlashga yordam beradi.

3. Shifrlashdan foydalaning. Aloqa tarmoqlari orqali uzatiladigan ma'lumotlarni shifrlash, hatto ushlangan taqdirda ham ruxsatsiz foydalanuvchilar uchun o'qib bo'lmasligini ta'minlaydi. AES 256-bit kabi kuchli shifrlash algoritmlari ruxsatsiz kirishdan ishonchli himoyani ta'minlaydi.

4. Intrusionlarni aniqlash va oldini olish tizimlarini joriy etish. Tashkilotlar tajovuzlarni aniqlash va oldini olish tizimlarini (IDPS) o'rnatish orqali tarmoqlarni proaktiv ravishda kuzatishi, shubhali harakatlarni aniqlashi va ruxsatsiz kirishlarning oldini olishi mumkin. IDPS potentsial tahdidlarni tezda aniqlashi va ularga javob berishi, muhim aloqa tarmoqlariga ta'sirini minimallashtirishi mumkin.

5. Muntazam xavfsizlik auditi va baholashlarini o'tkazish. Muntazam xavfsizlik auditlari va baholashlari aloqa tarmoqlaridagi zaiflik va zaif tomonlarni aniqlashga yordam beradi. To'liq baholashni o'tkazish orqali tashkilotlar ruxsatsiz bosqinlar tomonidan foydalanilgunga qadar mumkin bo'lgan xavfsizlik bo'shliqlarini bartaraf etishlari mumkin.

Sun'iy intellekt (AI) va Machine Learning (ML): AI va ML texnologiyalari tahdidlarni aniqlash va ularga javob berish imkoniyatlarini oshirishi mumkin, bu esa tashkilotlarga real vaqtda potentsial hujumlarni aniqlash va kamaytirish imkonini beradi.

Zero Trust Architecture: Zero Trust arxitekturasi har bir foydalanuvchi uchun doimiy autentifikatsiya va avtorizatsiyani talab qiladigan joylashuv yoki tarmoq segmentiga asoslangan ishonchni hech qachon qabul qilmaslik orqali muhim aloqa tarmoqlariga xavfsiz kirishni ta'minlashga qaratilgan.

Blokcheyn texnologiyasi: blokcheyn texnologiyasining markazlashtirilmagan tabiati muhim aloqa tarmoqlari uchun kengaytirilgan xavfsizlikni taklif qilishi mumkin, bu esa zararli shaxslarning ma'lumotlarni buzishi yoki ruxsatsiz kirishni qiyinlashtiradi.

Muhim aloqa tarmoqlarining xavfsizligini ta'minlash jismoniy shaxslar va tashkilotlar uchun ustuvor vazifa bo'lishi kerak. Rivojlanayotgan tahdidlar

manzarasini tushunish va samarali xavfsizlik strategiyalarini amalga oshirish orqali biz ruxsatsiz buzg'unlardan himoya qila olamiz va nozik ma'lumotlarni noto'g'ri qo'llarga tushishdan himoya qila olamiz.

Esda tutingki, kiberxavfsizlik doimiy sayohatdir va hushyor bo'lish muhim aloqa tarmoqlarining yaxlitligini saqlashning kalitidir.

Ruxsatsiz kirish tahdidining kuchayishi. Ruxsatsiz kirish deganda tegishli ruxsatsiz aloqa tizimlariga kirishga qaratilgan har qanday zararli urinish tushuniladi. Bunday ruxsatsiz kirish ma'lumotlarning buzilishi, shaxsiy hayotning buzilishi, moliyaviy yo'qotishlar va obro'ga putur etkazishi mumkin. Accenture tomonidan e'lon qilingan so'nggi hisobotga ko'ra, kelgusi besh yil ichida kiberjinoyat tashkilotlarga butun dunyo bo'ylab hayratlanarli 5,2 trillion dollarga tushadi.

Ushbu ortib borayotgan tahdidga qarshi turish uchun shaxslar va tashkilotlar o'zlarining aloqa tizimlarining xavfsizlik holatini mustahkamlovchi strategiyalarni faol ravishda amalga oshirishlari kerak. Bu yerda ko'rib chiqilishi kerak bo'lgan ba'zi asosiy choralar:

1. Kuchli autentifikatsiya mexanizmlarini amalga oshirish

Autentifikatsiya ruxsatsiz kirishning oldini olishda muhim rol o'ynaydi, bu foydalanuvchilarning o'zlari da'vo qilgan shaxs ekanligini ta'minlash. Ko'p faktorli autentifikatsiya (MFA) kabi zamonaviy autentifikatsiya mexanizmlari qo'shimcha xavfsizlik darajasini ta'minlaydi. Statistika shuni ko'rsatadiki, TIV hisobni o'zlashtirish xavfini 99,9% ga kamaytirishi mumkin. Kuchli autentifikatsiya mexanizmlarining ba'zi asosiy xususiyatlari va afzalliklari quyidagilardan iborat:

- Barmoq izi yoki yuzni tanish kabi biometrik ma’lumotlardan foydalaning
- Qo'shimcha xavfsizlik uchun noyob bir martalik kodlarni yarating
- Foydalanuvchi tajribasini yo'qotmasdan xavfsizlikni oshiring
- Hisob ma'lumotlari buzilgan taqdirda ham ruxsatsiz foydalanuvchilarning kirishini oldini oling

2. Shifrlash usullaridan foydalanish. Shifrlash aloqa tizimlarini himoya qilishning muhim jihati hisoblanadi, chunki u nozik ma'lumotlarni o'qib bo'lmaydigan formatga kodlash orqali himoya qiladi. Kuchli shifrlash usullarini qo'llash orqali ruxsatsiz shaxslar ushlangan ma'lumotlarni shifrlashni deyarli imkonsiz deb topadilar. Shifrlashning afzalliklari quyidagilardan iborat:

- Maxfiy ma'lumotlarga ruxsatsiz kirishni oldini olish
- Ma'lumotlarni himoya qilish qoidalariga rioya qilish

- O'tkazish yoki saqlash vaqtida ma'lumotlar maxfiyligini saqlash
- Mijozlarning nozik ma'lumotlarini himoya qiling va ishonchni mustahkamlash

3. Dasturiy ta'minotni muntazam yangilash va tuzatish. Dasturiy ta'minotning zaif tomonlari ruxsatsiz kirish uchun katta imkoniyatlar yaratadi. Xakerlar aloqa tizimlariga kirish uchun eskirgan dasturiy ta'minotning zaif tomonlaridan foydalanadilar. Dasturiy ta'minotni muntazam yamoqlar va yangilanishlar bilan yangilab turish juda muhimdir.

4. Mustahkam xavfsizlik devori yechimini joriy qilish

Xavfsizlik devori ichki tarmoq va tashqi dunyo o'rtasida to'siq bo'lib, kiruvchi va chiquvchi trafikni kuzatib boradi va nazorat qiladi. Kuchli xavfsizlik devorini joriy qilish orqali aloqa tizimlari ruxsatsiz kirish urinishlarini minimallashtirishi mumkin.

"Rolli metodi" (Role-Based Access Control, RBAC) - bu axborot tizimlaridagi foydalanuvchilar va resurslarga ruxsatni boshqarish uchun amal qiladigan usul. Bu usulda, har bir foydalanuvchi uchun bir yoki bir nechta rollar belgilanadi va har bir rolga mos keladigan huquqlar (ruxsatlar) aniqlanadi. Foydalanuvchilar o'z rollariga binoan huquqlarga ega bo'ladi. Roli metodi asosida ruxsatsiz foydalanishlarni kontrol qilishning bir nechta usullari mavjud. Bu usullardan bir qanchasi quyidagilar bo'lishi mumkin:

Rollarni aniqlash: Har bir foydalanuvchi uchun zarur rollarni aniqlash. Bu rollar, foydalanuvchining vazifalariga, maqsadiga va boshqa faktorlarga bog'liq bo'ladi. Masalan, "admin", "mudir" kabi.

Huquqlarni belgilash: Har bir rolni tushungan holda, ushbu rolni bajarish uchun kerak bo'lgan huquqlarni belgilash. Masalan, "fayllarni ko'rish", "ma'lumotlarni o'zgartirish", "foydalanuvchilarni qo'shish" kabi.

Foydalanuvchilar va rollar orasidagi bog'lanishlarni belgilash: Har bir foydalanuvchining bir yoki bir nechta rollarga ega bo'lishi mumkin. Rollar va foydalanuvchilar orasidagi bog'lanishlarni belgilash, foydalanuvchining barcha kerakli huquqlarni olishini ta'minlaydi.

Rollar va huquqlar bo'yicha ruxsatlarni boshqarish tizimi: Foydalanuvchilarni, rollarni va huquqlarni boshqarish uchun tizimni ishlab chiqish.

Bu tizim orqali adminstratorlar va boshqa shaxslar kerakli huquqlarni o'zgartirishlari mumkin bo'ladi.

Monitoring va logging: Tizimda amalga oshirilayotgan har xil amallarni monitoring qilish va logging (jarayonlarni kuzatish) tizimini o'rnatish. Bu tizimdagi har qanday ruxsatlarni nazorat qilish va aniq ma'lumotlar olishga yordam beradi.

Regulyar ravishda tekshiruvlar: Foydalanuvchilar, rollar va huquqlar tizimida o'zgarishlar bo'lsa, regulyar ravishda tekshiruvlar o'tkazish. Bu, xavfsizlikni ta'minlashda yordam beradi.

Bu usullar bir qator axborot tizimi xususiyatlari va kerakliliklariga bog'liq o'zgartirilishi mumkin. Har bir tizimning o'ziga xos tizim yaratish uchun bu usullarni adaptatsiya qilish muhimdir.

Asosiy xulosalar. Aloqa tizimlarini ruxsatsiz kirishdan himoya qilish bugungi raqamli aloqa dunyosida juda muhimdir. Kuchli autentifikatsiya mexanizmlarini joriy qilish, shifrlash usullarini qo'llash, dasturiy ta'minotni muntazam yangilash va ishonchli xavfsizlik devori yechimini joriy qilish orqali shaxslar va tashkilotlar ruxsatsiz kirish xavfini sezilarli darajada kamaytirishi va maxfiy ma'lumotlarini himoya qilishi mumkin.

FOYDALANILGAN ADABIYOTLAR:

1. И.М. Абдуллаева, Д.Т. Азимов. Ахборот тизимлари менежменти // Ўқув қўлланма // Тошкент – iqtisodiyot – 2019.
2. A.T. Kenjaboyev, m.yu. Jumaniyazova. Elektron biznes asoslari // O'quv qo'llanma. Toshkent. "Iqtisod-moliya" – 2008.
3. A.A. Akayev va boshqalar. Iqtisodiyotda axborot komplekslari va texnologiyalari // Darslik. Toshkent – 2019.
4. S.K. Ganiev, A.A. Ganiev, Z.T. Xudoyqulov. Kiberxavfsizlik asoslari // O'quv qo'llanma. Toshkent – 2020.
5. German M.V. va boshqalar. Elektron tijorat va biznes // O'quv qo'llanma. Samarqand – 2021.
6. Федорова Г.Н. Информатsионные системы // Учебник. Издательский центр «Академия». Москва – 2013.
7. И.Л. Чудинов, В.В. Осипова. Информатsионные системы и технологии // Учебное пособие. Издательство Томского политехнического университета – 2013.

8. Жданов С.А. и др. Информatsионные системы // Учебник для вузов. Изд.-во «Прометей», 2015.
9. Рудакова Е.В. Признаки, виды и особенности информatsионных систем // Журнал «Духовная ситуация времени. Россия XXI век». 3 (18) – 2019.
10. Sebastian K.Boell, Dubravka Cecez-Kecmanovic. What is an Information sistem? Conference: Proceedings of the 48th Hawaiian International Conference on System Sciences (HICSS), At: Kauaii, Hawaii, USA, 2015.
11. Https://www.simplilearn.com/types-of-information-systems-andapplications-article
12. https://lex.uz/docs/-5679590