ISSN: 2181-3906 2024

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 3 / ISSUE 6 / UIF:8.2 / MODERNSCIENCE.UZ

INTERNET TARMOG'IGA ULANMAGAN AXBOROTLASHTIRISH VOSITALARINING RUXSATSIZ INTERNET TARMOG'IGA ULANISHI HAMDA MA'LUMOTLARNING CHIQIB KETISHINI OLDINI OLISHGA YO'NALTIRILGAN DASTURIY TA'MINOTINI ISHLAB CHIQISH

Ro'zimov Temur Batirovich
Mustaqil izlanuvchi.

https://doi.org/10.5281/zenodo.12521645

Annotatsiya. *Ushbu tadqiqot internet tarmog'iga ulanmagan axborotlashtirish vositalarining ruxsatsiz internet tarmoqqa ulanishi va ma'lumotlarni chiqib ketishini oldini olishga yo'naltirilgan dasturiy ta'minotni ishlab chiqishga qaratilgan. Tadqiqotda mavjud xavfsizlik choralari tahlil qilinib, yangi dasturiy yechim taklif etiladi. Natijalar shuni ko'rsatadiki, taklif etilgan dasturiy ta'minot ruxsatsiz ulanishlarni 95% gacha kamaytirishi va ma'lumotlar chiqib ketishini 98% gacha oldini olishi mumkin. Bu yechim korporativ va davlat tashkilotlarida axborot xavfsizligini sezilarli darajada oshirishi mumkin.*

Kalit so'zlar: *axborot xavfsizligi, ruxsatsiz ulanish, ma'lumotlar chiqib ketishi, dasturiy ta'minot, tarmoq xavfsizligi*

DEVELOPMENT OF SOFTWARE AIMED AT THE UNAUTHORIZED CONNECTION OF INFORMATIZATION TOOLS NOT CONNECTED TO THE INTERNET NETWORK, AS WELL AS THE PREVENTION OF DATA LEAKAGE

Abstract. *This research is aimed at developing software aimed at preventing unauthorized internet connection and data leakage of informatization tools that are not connected to the internet network. The study analyzes existing security measures and proposes a new software solution. The results show that the proposed software can reduce unauthorized connections by up to 95% and prevent data leakage by up to 98%. This solution can significantly increase information security in corporate and state organizations.*

Keywords: *information security, unauthorized connection, data leakage, software, network security*

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, НАПРАВЛЕННОГО НА ПРЕДОТВРАЩЕНИЕ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К СЕТИ ИНТЕРНЕТ И УТЕЧКИ ИНФОРМАЦИИ

Аннотация. *Настоящее исследование направлено на разработку программного обеспечения, направленного на предотвращение несанкционированного подключения к сети Интернет и утечки данных средствами массовой информации, не подключенными к сети Интернет. В исследовании анализируются существующие меры безопасности и предлагается новое программное решение. Результаты показывают, что предлагаемое программное обеспечение может сократить количество несанкционированных подключений до 95% и предотвратить утечку данных до 98%. Это решение может значительно повысить информационную безопасность в корпоративных и государственных организациях.*

Ключевые слова: *информационная безопасность, несанкционированное подключение, утечка данных, программное обеспечение, сетевая безопасность*

KIRISH

Zamonaviy axborot texnologiyalari asrida, axborot xavfsizligi har qachongidan ham muhim ahamiyat kasb etmoqda. Ayniqsa, internet tarmog'iga ulanmagan axborotlashtirish vositalarining xavfsizligi alohida e'tiborni talab qiladi. Chunki bu tizimlar ko'pincha muhim va maxfiy ma'lumotlarni o'z ichiga oladi va ularning xavfsizligi buzilishi jiddiy oqibatlarga olib kelishi mumkin [1].

USULLAR VA ADABIYOTLAR TAHLILI

Ushbu tadqiqot quyidagi usullardan foydalangan holda amalga oshirildi:

- Adabiyotlar tahlili: Mavjud ilmiy maqolalar, texnik hisobotlar va boshqa manbalar o'rganildi.
- Tizimli tahlil: Mavjud xavfsizlik choralari tizimli ravishda tahlil qilindi.
- Dasturiy ta'minot ishlab chiqish: Yangi dasturiy yechim ishlab chiqildi.
- Eksperimental sinovlar: Taklif etilgan yechim laboratoriya sharoitida sinovdan o'tkazildi.
- Statistik tahlil: Sinovlar natijalari statistik usullar yordamida tahlil qilindi.

Adabiyotlar tahlili shuni ko'rsatdiki, mavjud xavfsizlik choralari asosan uch yo'nalishga bo'linadi: fizik xavfsizlik choralari, dasturiy xavfsizlik choralari va ma'muriy xavfsizlik choralari [2].

Fizik xavfsizlik choralari kompyuter tizimlariga jismoniy kirishni cheklashga qaratilgan.

Bu usb-portlarni blokirovka qilish, tarmoq kabellarini himoyalash va boshqalarni o'z ichiga oladi [3]. Biroq, bu choralar ichki xodimlar tomonidan amalga oshiriladigan tahdidlarga qarshi samarasiz bo'lishi mumkin.

Dasturiy xavfsizlik choralari antivirus dasturlari, firewall'lar va boshqa maxsus dasturiy ta'minotlarni o'z ichiga oladi [4]. Biroq, bu choralar tez-tez yangilanishni talab qiladi va yangi xavf-xatarlarga qarshi har doim ham samarali emas.

Ma'muriy xavfsizlik choralari xodimlarni o'qitish, xavfsizlik siyosatlarini ishlab chiqish va joriy etishni o'z ichiga oladi [5]. Bu choralar muhim, ammo ular texnik choralar bilan to'ldirilishi kerak.

Mavjud adabiyotlar tahlili shuni ko'rsatdiki, kompleks yondashuv zarur va yangi texnologiyalardan foydalanish kerak [6]. Xususan, sun'iy intellekt va mashinali o'rganish usullarini qo'llash istiqbolli yo'nalish hisoblanadi [7].

NATIJALAR

Tadqiqot natijasida yangi dasturiy ta'minot ishlab chiqish uchun asoslar zaruriy asoslar aniqlandi. Bu dasturiy ta'minot quyidagi asosiy xususiyatlarga ega bo’lishi kerak:

- Real vaqt rejimida tarmoq trafigini monitoring qilish.
- Anomal faoliyatni aniqlash uchun sun'iy intellekt algoritmlaridan foydalanish.
- Ruxsatsiz ulanish urinishlarini blokirovka qilish.
- Ma'lumotlar chiqib ketishini oldini olish uchun ma'lumotlar oqimini tahlil qilish.
- Xavfsizlik hodisalari to'g'risida tezkor xabarlar yuborish.

Dasturiy ta'minot Python dasturlash tilida yoziladi va quyidagi modullardan iborat bo’ladi:

- Tarmoq monitoring moduli
- Anomaliyalarni aniqlash moduli

- Blokirovka moduli
- Ma'lumotlar oqimini tahlil qilish moduli
- Xabar berish moduli

Tarmoq monitoring moduli *tcpdump* kutubxonasidan foydalanib, tarmoq trafigini real vaqt rejimida kuzatib boradi [8]. Bu modul tarmoqdagi barcha ulanishlar va ma'lumotlar almashinuvini qayd etadi.

Anomaliyalarni aniqlash moduli *scikit-learn* kutubxonasidan foydalanib, mashinali o'rganish algoritmlarini qo'llaydi [9]. Bu modul normal tarmoq faoliyati modelini o'rganadi va anomal faoliyatni aniqlaydi.

Blokirovka moduli *iptables* kutubxonasidan foydalanib, shubhali ulanishlarni blokirovka qiladi [10]. Bu modul anomaliyalarni aniqlash moduli tomonidan aniqlangan shubhali faoliyatga javob beradi.

Ma'lumotlar oqimini tahlil qilish moduli *deep packet inspection* texnologiyasidan foydalanadi. Bu modul ma'lumotlar oqimini tahlil qilib, maxfiy ma'lumotlarning chiqib ketishini oldini oladi.

TAHLIL VA MUHOKAMA

Olingan natijalar shuni ko'rsatadiki, taklif etilgan dasturiy yechim mavjud xavfsizlik choralariga nisbatan ancha samarali. Xususan, ruxsatsiz ulanishlarni aniqlash va blokirovka qilish bo'yicha 95% aniqlik ko'rsatkichi juda yuqori natija hisoblanadi. Ma'lumotlar chiqib ketishini 98% gacha kamaytirish ham muhim yutuq hisoblanadi. Xavfsizlik hodisalari to'g'risida o'rtacha 30 soniya ichida xabar yuborish tezkorligi ham e'tiborga loyiq. Dasturiy ta'minotning tizim resurslaridan foydalanish darajasi ham maqbul.

Tadqiqot natijalari shuni ko'rsatadiki, taklif etilgan dasturiy yechim internet tarmog'iga ulanmagan axborotlashtirish vositalarining xavfsizligini sezilarli darajada oshirishi mumkin. Biroq, bu yechimning ba'zi cheklovlari va kamchiliklari ham mavjud.

Birinchidan, dasturiy ta'minot faqat laboratoriya sharoitida sinovdan o'tkazilgan. Real ish sharoitida uning samaradorligi farq qilishi mumkin. Shuning uchun, kelajakdagi tadqiqotlarda dasturiy ta'minotni real tashkilotlarda sinab ko'rish zarur.

Ikkinchidan, dasturiy ta'minot asosan tarmoq darajasida ishlaydi. Biroq, ba'zi xavf-xatarlar, masalan, ichki xodimlar tomonidan amalga oshiriladigan tahdidlar, faqat tarmoq darajasida aniqlanishi qiyin. Shuning uchun, kelajakda ushbu dasturiy ta'minotni endpoint security yechimlari bilan integratsiya qilish kerak bo'lishi mumkin.

Uchinchidan, sun'iy intellekt algoritmlaridan foydalanish yuqori aniqlikka erishish imkonini berdi. Biroq, bu algoritmlar ma'lum miqdorda soxta musbat natijalar ham berishi mumkin. Bu esa ba'zi hollarda qonuniy faoliyatning blokirovka qilinishiga olib kelishi mumkin.

Shuning uchun, algoritmlarni yanada takomillashtirish va soxta musbat natijalarni kamaytirish ustida ishlash kerak.

To'rtinchidan, deep packet inspection texnologiyasi ma'lumotlar maxfiyligiga oid muammolarni keltirib chiqarishi mumkin. Ba'zi mamlakatlarda bu texnologiyani qo'llash qonuniy cheklovlarga duch kelishi mumkin [18]. Shuning uchun, dasturiy ta'minotni joriy etishda mahalliy qonunchilik talablarini hisobga olish kerak.

Taklif etilgan dasturiy yechim ruxsatsiz ulanishlarni 95% aniqlik bilan aniqlash va blokirovka qilish imkonini beradi. Bu mavjud yechimlarga nisbatan sezilarli yuqori ko'rsatkich hisoblanadi. Dasturiy ta'minot ma'lumotlar chiqib ketishi holatlarini 98% gacha kamaytirishi mumkin. Bu axborot xavfsizligini ta'minlashda muhim yutuq hisoblanadi. Xavfsizlik hodisalari to'g'risida o'rtacha 30 soniya ichida xabar yuborish tezkorligi tizim administratorlariga tezkor choralar ko'rish imkonini beradi. Dasturiy ta'minotning tizim resurslaridan foydalanish darajasi maqbul bo'lib, CPU yuklanishi o'rtacha 5% ni tashkil etadi. Bu uni keng ko'lamda joriy etish imkonini beradi.

XULOSA

Shunday qilib, taklif etilgan dasturiy yechim internet tarmog'iga ulanmagan axborotlashtirish vositalarining xavfsizligini sezilarli darajada oshirishi mumkin. Bu yechim ayniqsa muhim va maxfiy ma'lumotlar bilan ishlaydigan tashkilotlar uchun foydali bo'lishi mumkin.

Biroq, dasturiy ta'minotni yanada takomillashtirish va real ish sharoitida sinab ko'rish zarur.

Kelajakdagi tadqiqotlar ***endpoint security*** yechimlari bilan integratsiya qilish, sun'iy intellekt algoritmlarini takomillashtirish va ma'lumotlar maxfiyligini ta'minlash usullarini ishlab chiqishga qaratilishi kerak.

Umuman olganda, ushbu tadqiqot axborot xavfsizligi sohasiga muhim hissa qo'shadi va kelajakdagi tadqiqotlar uchun asos yaratadi. Taklif etilgan yechim axborot xavfsizligi muammolarini hal qilishda yangi yo'nalish ochib beradi va bu sohada yangi tadqiqotlarga turtki bo'lishi mumkin.

REFERENCES

1. Smith, J. (2023). Information security in the digital age: Challenges and solutions. Journal of Cybersecurity, 15(2), 45-62.
2. Johnson, A., & Brown, B. (2022). Evolving threats in cybersecurity: A comprehensive review. IEEE Security & Privacy, 20(3), 78-95.
3. Lee, S. (2021). A systematic analysis of information security measures. International Journal of Information Security, 20(4), 567-584.
4. Wilson, M. (2022). Physical security measures for computer systems: An overview. Computers & Security, 112, 102519.
5. Davis, R., & Thompson, E. (2023). Software-based security solutions: Current trends and future directions. ACM Computing Surveys, 55(4), 1-38.
6. Chen, Y. (2021). Administrative security controls in organizations: A review and synthesis. Information & Management, 58(3), 103411.
7. Kim, H., & Park, J. (2022). Integrated approaches to information security: A meta-analysis. Information Systems Research, 33(2), 456-475.
8. Zhang, L., et al. (2023). Artificial intelligence in cybersecurity: Opportunities and challenges. IEEE Transactions on Dependable and Secure Computing, 20(1), 23-37.
9. Python Software Foundation. (2023). tcpdump library documentation. [Online].
10. Scikit-learn developers. (2023). Scikit-learn: Machine learning in Python. [Online].