VEB SAYTLARNI XAVFSIZLIK DARAJALARINI OSHIRISH UCHUN MONITORING TIZIMINI ISHLAB CHIQISH

TATU Fergana Branch

Solijonov Ziyodaziz Sodiqjon ugli

TATU Fergana Branch Assistant

Umarov is the son of ***Abdumukhtor Makhammad***

Abstract: *Ushbu maqolada veb saytlarning xavfsizlik darajasini oshirish uchun samarali monitoring tizimini ishlab chiqish masalalari ko‘rib chiqilgan. Veb saytlar, ayniqsa, foydalanuvchilar tomonidan shaxsiy ma’lumotlar uzatilishi va onlayn tranzaksiyalar amalga oshirilishi sababli, kiberxavfsizlik tahdidlariga doimo duch keladi. Monitoring tizimi veb saytlarni turli xavf-xatarlar, shu jumladan, hujumlar, zaifliklar va noto‘g‘ri sozlamalardan himoya qilishga yordam beradi. Maqolada xavfsizlik tahlili, xakerlar tomonidan amalga oshiriladigan hujumlar, xatoliklarni aniqlash, va tizimni monitoring qilish uchun kerakli vositalar tahlil qilinadi. Monitoring tizimining dizayni, texnik yechimlar va real vaqt rejimida xavfsizlikni nazorat qilish usullari haqida batafsil ma’lumot beriladi. Ushbu tadqiqot veb saytlar uchun yuqori darajadagi xavfsizlikni ta’minlashga qaratilgan yangi yondashuvlarni taklif qiladi.*

Key words: *Veb sayt xavfsizligi, monitoring tizimi, kiberxavfsizlik, xavf-xatarlarni aniqlash, tarmoq monitoringi, xaker hujumlari, zaifliklarni tahlil qilish, xavfsizlikni nazorat qilish, real vaqt monitoringi, ma’lumotlarni himoya qilish*

Bugungi kunda veb saytlar insonlar va bizneslar uchun muhim axborot manbalariga aylangan, shuning uchun ular kiberxavfsizlik tahdidlariga nisbatan juda sezgir. Internet orqali amalga oshiriladigan onlayn tranzaksiyalar, shaxsiy ma’lumotlar almashinuvi va xizmatlar taqdimoti veb saytlarning xavfsizligini yanada muhimlashtiradi. Veb saytlar o‘zining funksionalligi va foydalanuvchilar bilan o‘zaro aloqasi orqali bir qator xavfsizlik muammolarini yuzaga keltiradi.

Masalan, ma’lumotlarning o‘g‘irlanishi, xakerlik hujumlari, veb saytlar tizimidagi zaifliklar va noto‘g‘ri konfiguratsiyalar foydalanuvchilarga jiddiy zarar yetkazishi mumkin. Veb saytlarni himoya qilishda asosiy vazifa bu tizimni real vaqt rejimida nazorat qilish va xavfsizlik darajasini doimiy ravishda oshirib borishdir. Buning uchun monitoring tizimlari ishlab chiqish zarur. Ushbu tizimlar xavfsizlik tahdidlarini oldindan aniqlash, xatoliklarni tahlil qilish, zaifliklarni aniqlash va veb saytga bo‘ladigan hujumlarni samarali tarzda to‘xtatish imkonini beradi. Monitoring tizimlari veb saytlar uchun yuqori darajadagi xavfsizlikni ta’minlashda muhim rol o‘ynaydi, chunki ular tizimning faoliyatini real vaqt rejimida tahlil qiladi va tezkor javob choralarini ko‘rish imkonini beradi.

Veb saytlar va onlayn tizimlar kiberxavfsizlik tahdidlariga doimo duch kelmoqda. Ushbu tahdidlar tizimning zaif joylaridan foydalanishni, ma'lumotlarni o'g'irlashni, xizmatni rad etish hujumlarini (DDoS) va boshqa xavflarni o'z ichiga oladi. Veb saytlarning xavfsizligini oshirishning samarali usullaridan biri bu monitoring tizimini joriy etishdir. Monitoring tizimi veb saytning xavfsizligini real vaqt rejimida nazorat qilishga, muammolarni tezda aniqlashga va ularga javob berishga yordam beradi.

Monitoring tizimining tuzilishi va maqsadi: Monitoring tizimining asosiy maqsadi veb saytning xavfsizligini oshirish uchun tizimni real vaqt rejimida kuzatib borishdir. Bunday tizimlar veb saytga bo‘ladigan har qanday noxush faoliyatni aniqlash uchun turli vositalar va metodologiyalarni o‘z ichiga oladi. Monitoring tizimlari xavfsizlikni yaxshilash uchun quyidagi asosiy funktsiyalarni bajaradi:

Xavf-xatarlarni aniqlash, Hujumlarni aniqlash, xatoliklarni aniqlash, audit va hisobot.

Xavfsizlikni monitoring qilish uchun vositalar: Veb sayt xavfsizligini ta’minlash uchun turli monitoring vositalari qo‘llaniladi. Ularning eng keng tarqalganlaridan biri bu Intrusion Detection Systems (IDS) va Intrusion Prevention Systems (IPS). IDS tizimi tarmoqdagi yoki serverdagi potentsial xavflarni aniqlaydi, IPS esa bu tahdidlarga qarshi avtomatik tarzda choralar

ko‘radi. Shuningdek, Security Information and Event Management (SIEM) tizimlari real vaqt monitoringini ta’minlaydi va xavfsizlik hodisalarini tahlil qilishda yordam beradi. Bu vositalar veb saytlarning xavfsizligini ta’minlashda asosiy rol o‘ynaydi.

Veb sayt xavfsizligini monitoring qilishda shifrlash va autentifikatsiya: Veb saytlarni xavfsiz qilishda shifrlash va autentifikatsiya juda muhim ahamiyatga ega. SSL/TLS protokollari internet orqali uzatiladigan ma'lumotlarni shifrlashda qo‘llaniladi. Bu protokollar foydalanuvchi va veb sayt o‘rtasidagi ma’lumot uzatishni himoya qiladi. Shuningdek, autentifikatsiya mexanizmlari (masalan, ikki faktorlu autentifikatsiya) tizimga kirishni faqat muvofiqlashtirilgan foydalanuvchilarga cheklashda yordam beradi. Monitoring tizimi shifrlangan aloqalarni va autentifikatsiya jarayonlarini doimiy ravishda nazorat qiladi, shuningdek, tizimga nisbatan har qanday kirish harakatini qayd etadi.

DDoS hujumlari va xavfsizlik tahlili; DDoS hujumlari (Distributed Denial-of-Service) veb saytlar uchun eng katta xavflardan biri hisoblanadi. Bu hujumlar tizimni ish faoliyatidan chiqarish, xizmatni rad etish va foydalanuvchilarni saytga kira olishidan mahrum etish uchun amalga oshiriladi. DDoS hujumlarini aniqlash uchun monitoring tizimlari trafikni kuzatib boradi, zararli so‘rovlarni tahlil qiladi va tashqi tarmoqlardan kelayotgan ko‘p miqdordagi so‘rovlarni aniqlashga yordam beradi. Monitoring tizimi DDoS hujumlari haqida ogohlantirishlar yuborishi, hujumni to‘xtatish uchun avtomatik choralar ko‘rishi mumkin.

Monitoring tizimi orqali xatoliklarni bartaraf etish va o‘rganish: Monitoring tizimining yana bir muhim funksiyasi bu tizimda yuzaga kelgan xatoliklarni aniqlash va ularni bartaraf etishdir. Har qanday tizim xatoligi yoki noxush harakat tizimning xavfsizlik darajasini pasaytirishi mumkin. Monitoring tizimi bunday xatoliklarni aniqlab, administratorlarni ogohlantiradi va tizimni tezda tiklash imkonini beradi. Bundan tashqari, xatoliklarni tahlil qilish orqali yangi zaifliklar va ehtimoliy hujumlar haqida ma’lumot to‘plangan bo‘ladi, bu esa kelajakda xavfsizlikni yanada kuchaytirish imkonini beradi.

Real vaqt monitoringi va tizimni doimiy yangilash: Veb saytlarning xavfsizligini ta’minlashda eng muhim omillardan biri bu tizimning doimiy monitoringini olib borishdir. Real vaqt monitoringi xavfsizlik hodisalariga tezda javob berishga imkon beradi. Bundan tashqari, tizimni yangilab turish, xavfsizlikni oshirish va yangi tahdidlarga qarshi choralar ko‘rish zarur. Monitoring tizimi yordamida tizimdagi barcha o‘zgarishlar va zaifliklar doimiy ravishda kuzatib boriladi va tarmoq xavfsizligi ta’minlanadi.

Monitoring tizimining samaradorligini oshirish uchun takliflar: Monitoring tizimini samarali ishlashini ta’minlash uchun bir qator yondashuvlar mavjud. Avvalo, tizimni doimiy ravishda yangilab turish va xavfsizlikni oshiruvchi yangi texnologiyalarni qo‘llash zarur. Tizimga ko‘proq resurs ajratish va xatoliklar va zaifliklarni aniqlash uchun qo‘shimcha monitoring vositalarini o‘rnatish ham samarali yechimdir. Shuningdek, veb saytlarni himoya qilishda foydalanuvchilarga xavfsizlik bo‘yicha ta’lim berish va tizimdagi xavfsizlik hodisalariga tezkor javob berish uchun maxsus jamoalarni shakllantirish muhimdir.

FOYDALANILGAN ADABIYOTLAR

1. Tojimatov, D. X. (2022). Kiberxavfsizlik: tahdilar, muammolar, yechimlar, “. Axborot-kommunikatsiya texnologiyalari va telekommunikatsiyalari sohasida zamonaviy muammolar va yechimlar” Respublika Ilmiy-texnik anjumani TATU Farg ‘ona filiali.

2. Muxammadovich, M. F., & Maxammad o’g’li, U. A. (2022, November). AXBOROTNI XIMOYALASH TIZIMINI ISHLAB CHIQISH. In Proceedings of International Educators Conference (Vol. 1, No. 2, pp. 187-190).

3. Умаров, А. (2023, November). ИНТЕГРИРОВАННЫЙ ПОДХОД К ПРЕПОДАВАНИЮ КРИПТОГРАФИИ И КИБЕРБЕЗОПАСНОСТИ В ВУЗАХ: ТЕОРИЯ И ПРАКТИКА. In Conference on Digital Innovation:" Modern Problems and Solutions".

ISSN 3060-4567

4. Tojimatov, D. (2023, October). VR/AR TEXNOLOGIYALARINI KIBERXAVFSIZLIK SOHASIDA QO ‘LLASHNING DOLZARBLIGI. In Conference on Digital Innovation:" Modern Problems and Solutions".

5. Умаров, А. (2023, November). ПРОЕКТНАЯ МЕТОДИКА В ПРЕПОДАВАНИИ КРИПТОГРАФИИ: РАЗВИТИЕ ТВОРЧЕСКИХ И КОММУНИКАТИВНЫХ НАВЫКОВ. In Conference on Digital Innovation:" Modern Problems and Solutions".

6. Tojimatov, D. X. (2023). KIBERTAHDIDLARNI OLDINI OLISHDA KIBERRAZVEDKA AMALIYOTI VA UNING USTUVOR VAZIFALARI. Al-Farg’oniy avlodlari, 1(4), 82-85.

7. Umarov, A. (2023, November). Bulutli ma'lumotlarni himoya qilish: ma'lumotlar xavfsizligini ta'minlash. In Conference on Digital Innovation:"

8. Umarov, A. M. O. G. L. (2021). AXBOROT XAVFSIZLIGI XAVFINI BAHOLASH. Scientific progress, 2(8), 293-300.

9. Muxammadovich, M. F., & Maxammad o’g’li, U. A. Ro’zaliyev Abdumalikjon Vahobjon o’g’li.(2022). AXBOROTNI XIMOYALASH.