MA'LUMOTLAR MARKAZLARIDA XAVFSIZLIK TAHDIDLARI VA ULARNI HAL QILISH

Babakulov Bekzod Mamatkulovich o‘g‘li
Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universiteti Jizzax filiali o’qituvchisi
babakulov.bekzod23@gmail.ru
Sodiqov Diyorbek Sodiq o’g’li
Mirzo Ulug’bek nomidagi O‘zbekiston Milliy universiteti Jizzax filiali Axborot xavfsizligi (sohalar bo‘yicha) 3-kurs talabasi
diyorsodiqov67@gmail.com
tel: +998932797755

Annotatsiya: Ushbu maqolada ma'lumotlar markazlari va ularning xavfsizligini ta'minlashga bag'ishlangan. Unda zamonaviy infratuzilmaning ahamiyati, tamoyillari hamda ushbu markazlar duch keladigan asosiy xavfsizlik tahdidlari tahlil qilinadi. Maqolada ichki va tashqi xavflar, xususan zararli dasturlar, DDoS hujumlari, insayder tahdidlari va kiberxavfsizlik bilan bog'liq boshqa muammolar yoritilgan. Ma'lumotlar markazlarini himoya qilish uchun IoT, VPN, ma'lumotlarni shifrlash kabi zamonaviy texnologiyalar va usullar taqdim etilgan. Shuningdek, gibrid tizimlar, tarmoq segmentatsiyasi va xavfsizlik devorlari orqali xavfsizlikni oshirish bo‘yicha yondashuvlar tavsiya etiladi. Dinamik falokatlarni tiklash, zaxira rejalarini ishlab chiqish, xodimlarning xavfsizlik xabardorligini oshirish kabi chora-tadbirlar ko‘rib chiqilgan. Maqolada nafaqat kiberhujumlarning oldini olish, balki ma'lumotlarning uzluksizligini ta'minlashga ham qaratilgan. Ushbu yechimlar kiberxavfsizlikning dolzarbligi oshib borayotgan bir paytda, tashkilotlar uchun katta ahamiyatga ega.

Kalit so’zlar: ma'lumotlar markazi, xavfsizlik tahdidlari, kiberxavfsizlik, zararli dasturlar, DDoS hujumlari, insayder tahdidlar, ma'lumotlarni shifrlash, IoT xavfsizligi, VPN, gibrid infratuzilma, zaxira rejalar, normativ muvofiqlik, API xavfsizligi, ransomware, autentifikatsiya tizimlari, ma'lumotlar maxfiyligi, ichki xavflar, texnologik yechimlar, xavfsizlik siyosati, DevSecOps, AI va ML, monitoring tizimlari, falokatni tiklash.

SECURITY THREATS IN DATA CENTERS AND THEIR SOLUTIONS

Abstract: AnnotThis article is dedicated to data centers and their security. It analyzes the importance, principles, and key security threats faced by these centers. The work covers internal and external threats, including malware, DDoS attacks, insider threats, and other cybersecurity issues. Modern technologies and methods for protecting data centers, such as IoT, VPN, and data encryption, are presented. It also recommends approaches to increasing security through hybrid systems, network segmentation, and firewalls. Measures such as dynamic disaster recovery, developing backup plans, and increasing employee security awareness are considered. The article focuses not only on preventing cyberattacks,

but also on ensuring data continuity. These solutions are of great importance for organizations as cybersecurity becomes increasingly relevant.

Keywords: data center, security threats, cybersecurity, malware, DDoS attacks, insider threats, data encryption, IoT security, VPN, hybrid infrastructure, backup plans, regulatory compliance, API security, ransomware, authentication systems, data privacy, insider risks, technology solutions, security policy, DevSecOps, AI and ML, monitoring systems, disaster recovery.

УГРОЗЫ БЕЗОПАСНОСТИ В ДАТА-ЦЕНТРАХ И ИХ РЕШЕНИЯ

Абстрактный: Аннотация Эта статья посвящена дата-центрам и их безопасности. В нем анализируются важность и принципы современной инфраструктуры, а также основные угрозы безопасности, с которыми сталкиваются эти центры. В деле рассматриваются внутренние и внешние угрозы, в частности вредоносное ПО, DDoS-атаки, внутренние угрозы и другие проблемы кибербезопасности. Для защиты дата-центров представлены современные технологии и методы, такие как IoT, VPN, шифрование данных. Также рекомендуются подходы к повышению безопасности с помощью гибридных систем, сегментации сети и межсетевых экранов. Были рассмотрены такие меры, как динамическое аварийное восстановление, разработка планов резервного копирования и повышение осведомленности сотрудников о безопасности. В статье основное внимание уделяется не только предотвращению кибератак, но и обеспечению непрерывности данных. Эти решения представляют большую ценность для организаций в то время, когда кибербезопасность становится все более важной.

Ключевые слова: центр обработки данных, угрозы безопасности, кибербезопасность, вредоносное ПО, DDoS-атаки, инсайдерские угрозы, шифрование данных, безопасность IoT, VPN, гибридная инфраструктура, планы резервного копирования, соответствие нормативным требованиям, безопасность API, программы-вымогатели, системы аутентификации, конфиденциальность данных, инсайдерские риски, технологические решения, политика безопасности, DevSecOps, AI и ML, системы мониторинга, аварийное восстановление.

KIRISH

Ma'lumotlar markazlari bugungi raqamli iqtisodiyotning yuragi bo‘lib, korxona va tashkilotlarning kundalik faoliyatida muhim ahamiyatga ega. Bu markazlar ulkan hajmdagi ma'lumotlarni saqlash, qayta ishlash va uzatish uchun mo‘ljallangan bo‘lib, ular nafaqat iqtisodiy samaradorlikni oshiradi, balki strategik qarorlarni qabul qilish uchun ham asos bo‘lib xizmat qiladi. Ammo, bu markazlarning jadal rivoji va ularga bo‘lgan qaramlik ortishi bilan xavfsizlikka oid yangi tahdidlar ham yuzaga kelmoqda.

Kiberhujumlar, tabiiy ofatlar, ichki xodimlarning xatolari yoki zararli niyatlari ma'lumotlar markazlariga sezilarli zarar yetkazishi mumkin. Ayniqsa, kiberxavfsizlik sohasida tahdidlar tobora murakkablashib borayotgan bir paytda, ushbu tahdidlarni

aniqlash, ularga qarshi choralar ko‘rish va ularni hal qilish bo‘yicha innovatsion yondashuvlar zarur. Shu sababli, ma'lumotlar markazlarida xavfsizlikni ta'minlash faqat texnologik yechimlarni emas, balki samarali boshqaruvni, xodimlarni o‘qitishni va zamonaviy xavfsizlik strategiyalarini ham o‘z ichiga oladi.

Mazkur maqolada ma'lumotlar markazlarida uchraydigan asosiy xavfsizlik tahdidlarini tahlil qilish va ularga qarshi samarali yechimlarni ishlab chiqish masalalari ko‘rib chiqiladi. Shu bilan birga, so‘nggi texnologiyalar va xalqaro tajribalardan foydalanish orqali ushbu muammolarning yechimlariga yondashish yo‘llari yoritiladi.

Ma'lumotlar markazlari duch keladigan xavfsizlik tahdidlarining turlari

Ma'lumotlar markazlari o'z faoliyatini xavf ostiga qo'yadigan ko'plab xavfsizlik tahdidlariga duch keladi. Zararli dasturlar, to'lov dasturlari va DDoS hujumlari kabi kiberhujumlar keng tarqalgan. Ular xizmatlarni buzishi va maxfiy ma'lumotlarni o'g'irlashi mumkin. Ushbu hujumlar ko'pincha murakkab va ularga qarshi kurashish uchun ilg'or xavfsizlik choralarini talab qiladi.

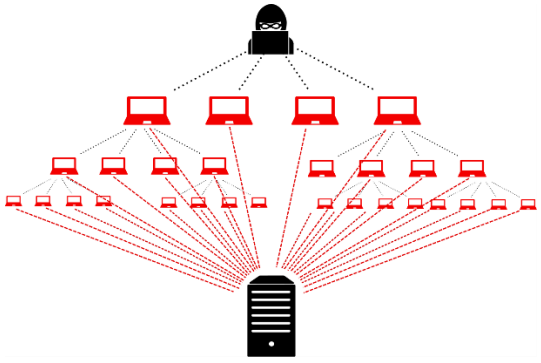
Ichki tahdidlar ham katta xavf tug'diradi. Yomon niyatli xodimlar yoki pudratchilar katta zarar yetkazishi mumkin. Bu bunday faoliyatni aniqlash va oldini olish uchun kuchli kirishni boshqarish va monitoring tizimlariga ega bo'lish juda muhim .

O'g'irlik, vandalizm va tabiiy ofatlar kabi jismoniy tahdidlar ma'lumotlar markazi xavfsizligiga ta'sir qilishi mumkin. Kuzatuv va kirishni boshqarish kabi kuchli jismoniy xavfsizlik choralari muhim ahamiyatga ega. Ushbu tahdidlarni tushunish keng qamrovli xavfsizlik strategiyasini ishlab chiqish uchun kalit hisoblanadi.

DDoS hujumi

Serverlar DDoS hujumining asosiy nishoni bo‘lib, muhim internet xizmatlarini buzish va o‘chirish uchun mo‘ljallangan.

Xizmatning mavjudligi ijobiy mijozlar tajribasi uchun juda muhimdir. Biroq, DDoS hujumlari mavjudlikka to'g'ridan-to'g'ri tahdid solishi mumkin, natijada biznes daromadlari, mijozlari va obro'si yo'qoladi. 2011 yildan 2013 yilgacha DDoS hujumlarining o'rtacha hajmi 4,7 Gbit / s dan 10 Gbit / s gacha ko'tarildi. Eng yomoni, odatiy DDoS hujumi paytida soniyasiga o'rtacha paketlar sonining hayratlanarli darajada o'sishi ham kuzatildi.



1-rasm. DDoS hujumi

Bu DDoS hujumlarining tez o'sishi ko'pgina standart tarmoq uskunalarini o'chirish uchun yetarli ekanligini isbotladi. Buzg'unchilar DDoS hujumlarining ko'lami va

intensivligini birinchi navbatda Web, DNS va NTP serverlaridan foydalanish orqali kuchaytirishi mumkin, bu esa korxonalardan har doim tarmoq monitoringini yaxshi bajarishni talab qiladi.

Veb-ilovaga hujum

Veb-ilovalar SQL iny'ektsiyasi, saytlararo skriptlar, saytlararo so'rovlarni qalbakilashtirish va h.k. kabi bir qator hujumlarga nisbatan zaifdir. Hujumchilar foyda olish maqsadida ilovalarga kirishga va ma'lumotlarni o'g'irlashga urinishadi, bu esa korxonalarning ma'lumotlar zaifligiga olib keladi. 2015 yilgi Trustwave Global xavfsizlik hisobotiga ko'ra, ilovalarning taxminan 98% zaifliklarga ega yoki bo'lgan. Buzg'unchilar tobora zaif veb-serverlarni nishonga olishmoqda va ularni DDoS hujum manbasiga aylantirish uchun zararli kodlarni o'rnatmoqdalar. Korxonalar veb-hujumlarni to'xtatish va ma'lumotlar zaifliklarini "virtual tuzatish" uchun proaktiv himoyaga muhtoj. Veb-ilovalar bir qator hujumlarga, jumladan OWASP Top 10 va CWE Top 25 ta eng xavfli dasturiy ta'minotning zaif tomonlarida ko'rsatilgan hujumlarga nisbatan zaifdir.

DNS hujumlari

DNS infratuzilmasi DDoS hujumlari yoki boshqa tahdidlarga ham zaifdir. U ikki sababga ko'ra ma'lumotlar markazining kiberhujumlari nishoniga aylanadi. Birinchidan, tajovuzkorlar turli xil vositalar orqali DNS-serverlarni oflayn rejimga o'tkazish orqali Internet foydalanuvchilarining Internetga kirishini oldini olishlari mumkin. Agar tajovuzkor internet-provayderning DNS-serverlarini o'chirib qo'ysa, ular Internet-provayderning foydalanuvchilarga va Internet xizmatlariga qilgan barcha ishlarini bloklashi mumkin. Ikkinchidan, tajovuzkorlar DNS serverlaridan foydalanish orqali DDoS hujumlarini ham kuchaytirishi mumkin. Buzg'unchilar o'zlarining haqiqiy maqsadlarining IP manzillarini aldashadi, DNS serverlariga ko'plab DNS serverlarini rekursiv ravishda so'rashni yoki qurbonlarga javoblar oqimini yuborishni buyuradilar. Bu DNS serveriga qurbonning DNS-trafik tarmog'ini bevosita boshqarish imkonini beradi. DNS server tajovuzkorlar uchun yakuniy maqsad bo'lmasa ham, u DNS aks ettirish hujumlari tufayli ma'lumotlar markazining ishlamay qolishi va uzilishlariga olib keladi.

Normativ muvofiqlik va kiberhujumlarning oldini olish strategiyalari

Raqamli infratuzilmaga bo'lgan ishonch ortib borayotgani sababli ma'lumotlar markazi xavfsizligi muhim ahamiyatga ega. Korxonalar ko‘proq IoT qurilmalari va bulutli yechimlardan foydalanar ekan, saqlanadigan va qayta ishlanadigan ma’lumotlar miqdori tez o‘sib boradi. Ushbu ma'lumotlarni himoya qilish ma'lumotlar buzilishi va kiberhujumlarning oldini olish uchun juda muhimdir. Bunday hodisalar jiddiy oqibatlarga olib kelishi mumkin. Ma'lumotlar markazlaridagi xavfsizlik muammolari katta moliyaviy yo'qotishlar, obro'ga putur yetkazishi va qonuniy javobgarlikka olib kelishi mumkin.

2-rasm. Kiber tahdidlarning oldini olish uchun qonunchilik bazasi va ilg'or himoya vositalarini integratsiyalash

Ruxsatsiz kirishning oldini olish va ma'lumotlar yaxlitligi va mavjudligini ta'minlash uchun kuchli xavfsizlik choralari zarur. Ma'lumotlar markazlari ko'pincha kompaniya faoliyatining asosi hisoblanadi.

Normativ muvofiqlik ko'pincha qat'iy xavfsizlik protokollarini talab qiladi. Ma'lumotlar markazi xavfsizligini tushunish operatsion samaradorlikni saqlash uchun zarurdir.14 xil sanoat sektoridagi 49 ta AQSH kompaniyasi ishtirok etgan. Ma’lumotlar buzilishining narxi so‘roviga ko‘ra , ular quyidagilarni payqashdi:

- ✓ Kompaniyalarning 39 foizi e'tiborsizlik ma'lumotlar buzilishining asosiy sababi ekanligini aytishdi
- ✓ Yomon yoki jinoiy hujumlar umumiy buzilishlarning 37 foizini tashkil qiladi.
- ✓ Buzilishning o'rtacha qiymati 5,5 million dollarni tashkil qiladi.

Hozirgi kunda ko'plab yirik kompaniyalar o'zlarining va mijozlarining ma'lumotlarini saqlash uchun bulutdan foydalanmoqdalar, ammo bulutda ma'lumotlarni saqlash xavfi juda katta bo'lishi mumkin. Kiberhujumlar ko'plab kompaniyalar uchun juda zararli bo'lishi mumkin. Dunyo bo'ylab kompaniyalarning 64 foizi faqatgina 2020 yilda kiberhujumlar bilan bog'liq muammolarga duch kelgan. Shaxsiy ma'lumotlarni o'g'irlash kabi ba'zi kiber hujumlar hayotni o'zgartiruvchi ta'sirlar bilan kimningdir kreditlariga zarar yetkazishi mumkin.

Ma'lumotlar markazi xavfsizligini ta'minlashning innovatsion yechimlari

Ma'lumotlar markazlari tashkilot IT infratuzilmasining eng muhim qismlaridan biridir.Ma'lumotlar markazi faoliyatining buzilishi biznesning ishlash qobiliyatiga sezilarli ta'sir ko'rsatadi. Ma'lumotlar markazlarining (va ularda joylashgan ma'lumotlar va ilovalar) mavjudligi va xavfsizligiga ikkita asosiy tahdid - bu asosiy infratuzilmaga tahdidlar va ushbu infratuzilmada joylashgan ma'lumotlar va ilovalarga kiber tahdidlar.

Infratuzilmaga to'g'ridan-to'g'ri hujumlar

Ma'lumotlar markazlari uch turdagi komponentlardan iborat: hisoblash, saqlash va tarmoq funksionalligi. Ushbu infratuzilmaga qarshi ekspluatatsiyalar ma'lumotlar markazining mavjudligi, ishlashi va xavfsizligiga ta'sir qiladi.

Ma'lumotlar markazlari infratuzilma ekspluatatsiyasiga qarshi turli xil himoya vositalarini o'z ichiga olishi uchun mo'ljallangan. Muhim funksiyalar uchun ortiqcha foydalanish bitta nosozlik nuqtalarini bartaraf etishga va ish vaqtini maksimal darajada oshirishga yordam beradi. Bu tajovuzkorlar uchun ushbu infratuzilmada joylashgan ilovalarni buzishni qiyinlashtiradi.

Bundan tashqari, ma'lumotlar markazlarida tabiiy hodisalar va xizmatlarga kirishni buzishi mumkin bo'lgan hujumlarni bartaraf etish uchun mo'ljallangan qo'llab-quvvatlash infratuzilmasi mavjud. Bularga uzluksiz quvvat manbalari (UPS), yong'inni o'chirish tizimlari, iqlim nazorati va bino xavfsizligi tizimlari kiradi.

Ma'lumotlar markazining xavfsizligini ta'minlash jarayoni tizimni tahlil qilishning kompleks yondashuvini va ma'lumotlar markazi rivojlanishi bilan xavfsizlik darajasini yaxshilaydigan doimiy jarayonni talab qiladi. Yangi ilovalar yoki xizmatlar paydo bo'lishi bilan ma'lumotlar markazi doimiy ravishda rivojlanmoqda. Hujumlar yanada murakkab va tez-tez bo'lib bormoqda. Ushbu tendentsiyalar xavfsizlikning tayyorligini barqaror baholashni talab qiladi.

Ma'lumotlar markazlarining asosiy mas'uliyati xizmatlarning mavjudligiga ishonch hosil qilish bo'lganligi sababli, ma'lumotlar markazini boshqarish tizimlari ko'pincha uning xavfsizligi trafik oqimlari, nosozliklar va kengaytirilishiga qanday ta'sir qilishini ko'rib chiqadi. Xavfsizlik choralari ma'lumotlar markazi dizayniga, noyob xususiyatlardan foydalanishga, muvofiqlik talablariga yoki kompaniyaning biznes maqsadlariga qarab farq qilishi mumkinligi sababli, barcha mumkin bo'lgan senariylarni qamrab oluvchi aniq chora-tadbirlar to'plami mavjud emas.

Ma'lumotlar markazi xavfsizligi ilovalar, infratuzilma, ma'lumotlar va foydalanuvchilarni himoya qilish uchun jismoniy ma'lumotlar markazlari va ko'p bulutli muhitlardagi ish yukini kuzatib boradi.Amaliyot jismoniy serverlarga asoslangan an'anaviy ma'lumotlar markazlaridan virtuallashtirilgan serverlarga asoslangan zamonaviyroq ma'lumotlar markazlariga nisbatan qo'llaniladi. Bu ommaviy bulutdagi ma'lumotlar markazlariga ham tegishli.

Umuman olganda, ma'lumotlar markazi xavfsizligining ikki turi mavjud: jismoniy xavfsizlik va virtual xavfsizlik.

Jismoniy xavfsizlik

Ma'lumotlar markazining jismoniy xavfsizligi - bu ma'lumotlarni saqlaydigan mashinalarga har qanday jismoniy zarar yetkazilishining oldini olish uchun ma'lumotlar markazi ob'ektlariga o'rnatilgan protokollar to'plami.Ushbu protokollar tabiiy ofatlardan tortib korporativ josuslik va terroristik hujumlargacha bo'lgan hamma narsani hal qila olishi kerak.

Jismoniy hujumlarning oldini olish uchun ma'lumotlar markazlari quyidagi usullardan foydalanadi:

- ✓ CCTV xavfsizlik tarmog'i: 90 kunlik videoni saqlashga ega joylar va kirish nuqtalari.
- ✓ Tarmoq operatsiyalari markazi (MOK) Xizmatlar va texnik guruh

- ✓ Orqaga o'tishga qarshi / orqaga o'tishga qarshi turniket eshigi. Autentifikatsiyadan keyin faqat bir kishiga o'tishga ruxsat beradi.
- ✓ Birgalikda joylashgan ob'ektga bitta kirish nuqtasi.
- ✓ Alohida ma'lumot zallari, suitlar va katakchalar orqali trafikni minimallashtirish.
- ✓ Shaxsiy kataklarga kirishni cheklash
- ✓ Uch faktorli autentifikatsiya
- ✓ SSAE 16 ga mos ob'ektlar.
- ✓ Amaldagi apparatning kelib chiqishi va dizaynini tekshirish
- ✓ Faoliyatni kuzatish va ularning hisob ma'lumotlarini xavfsiz saqlash orqali insayder xavfini kamaytirish
- ✓ Hududlangan quruq quvurli purkagich bilan yong'inning oldini olish
- ✓ Tabiiy ofat xavfi bo'lmagan joylar

Virtual xavfsizlik

Virtual xavfsizlik - bu ma'lumotlar markazlari tomonidan serverlarda saqlangan ma'lumotlarning yaxlitligi, mavjudligi yoki maxfiyligiga ta'sir qiladigan masofadan ruxsatsiz kirishning oldini olish uchun o'rnatilgan xavfsizlik choralari.

Virtual yoki tarmoq xavfsizligini hal qilish qiyin vazifa, chunki unga hujum qilishning ko'plab usullari mavjud. Eng yomoni shundaki, u yildan-yilga rivojlanib bormoqda. Masalan, tajovuzkor ma'lumotlarga kirish uchun turli xavfsizlik devorlarini chetlab o'tish uchun zararli dasturdan (yoki shunga o'xshash ekspluatatsiyalardan) foydalanishga qaror qilishi mumkin. Eski tizimlar, shuningdek, xavfsizlikni xavf ostiga qo'yishi mumkin, chunki ularda ma'lumotlar xavfsizligining zamonaviy usullari mavjud emas.

O'tkazish paytida og'ir ma'lumotlarni shifrlash : veb-ilovalar uchun 256-bit SSL shifrlash. Ma'lumotlarni uzatish uchun 1024-bit RSA ochiq kalitlari. Fayllar va ma'lumotlar bazalari uchun AES 256-bit shifrlash.

- ✓ Barcha foydalanuvchilarning audit faoliyatini jurnallar.
- ✓ Himoyalangan foydalanuvchi nomlari va parollar: 256-bitli SSL orqali shifrlangan, murakkab parollar uchun talablar, rejalashtirilgan amal qilish muddatini sozlash, parolni qayta ishlatishning oldini olish.
- ✓ Tozalash darajasiga qarab kirish.
- ✓ AD/LDAP integratsiyasi.
- ✓ IP manzillar asosida boshqarish.
- ✓ Har bir noyob foydalanuvchini aniqlash uchun seans identifikatori cookie-fayllarini shifrlash.
- ✓ Ikki faktorli autentifikatsiya mavjudligi.
- ✓ Uchinchi tomon kirish testi har yili o'tkaziladi
- ✓ Xavfsizlik devorlari va avtomatlashtirilgan skaner orqali zararli dasturlarning oldini olish

Ma'lumotlar markazida tarmoq xavfsizligini himoya qilish juda muhim. Ma’lumotlar markazlari tarmog‘i xavfsizligiga beshta asosiy tahdidlar keltirib

chiqaradigan ma’lumotlar zaifliklari va tarmoq xavfsizligi xavflarini hisobga olgan holda, bu yerda ba’zi mudofaa yechimlari keltirilgan.

***Zaifliklarning oldini olish*:** tez-tez zaif bo'lgan tizimlar va ilovalarni himoya qilish va tuzatish uchun IPS ni o'rnating. IPS, shuningdek, DNS infratuzilmasiga qaratilgan ekspluatatsiyalarni yoki xavfsizlik himoyasidan qochish uchun DNS dan foydalanishga urinishlarni ham aniqlay oladi.

***Tarmoq segmentatsiyasi*:** samarali amalga oshirilgan tarmoq segmentatsiyasi lateral harakatlanishning oldini oladi va nol ishonchli xavfsizlik modeli ostida eng kam imtiyozlarga ega bo'ladi.

***Ilova va API himoyasini o'rnatish*:** Veb-ilovalar uchun OWASP 10 ta xavf-xatarini yumshatish yechimi veb va API xavfsizlik ilovalaridan foydalanishdir. Shuningdek, ma’lumotlar markazlari korxonalarga ichki tarmoqqa yetib borgunga qadar trafikni kuzatish va tekshirishga yordam berish uchun xavfsizlik devorlari va tajovuzlarni aniqlash tizimlarini (IDS) o‘rnatishi mumkin.

***DDoS ga qarshi himoya*:** DDoS tahdidlarini yumshatish uchun mahalliy va bulutli DDoS himoyasidan foydalaning.

***Hisob ma'lumotlarini o'g'irlashning oldini olish*:** Hisob ma'lumotlarini o'g'irlash hujumlarining oldini olish uchun foydalanuvchilar uchun fishingga qarshi himoyani o'rnating.

***Ta'minot zanjirlarini himoya qilish*:** AI va ML tomonidan qo'llab-quvvatlanadigan tahdidlarning oldini olish, shuningdek, EDR va XDR texnologiyalaridan foydalangan holda murakkab ta'minot zanjiri hujumlarini aniqlash va oldini olish.

Ma'lumotlar markazining xavfsizlik choralar tahlili

Turli xil xavfsizlik choralarini qo'llash ma'lumotlar markazlarini himoya qilish uchun juda muhimdir. Ushbu chora-tadbirlarni jismoniy, tarmoq va ma'lumotlarni shifrlash va uzatish xavfsizligiga keng ajratish mumkin.

Ma'lumotlar markazi infratuzilmasini himoya qilish uchun jismoniy xavfsizlik choralari zarur. Ushbu choralar ob'ektga nazorat ostida kirishni, kuzatuv tizimlarini va xavfsizlik xodimlarini o'z ichiga oladi. Jismoniy kirishni cheklash orqali siz ruxsatsiz shaxslarning nozik hududlarga kirishini oldini olishingiz mumkin.

Ma'lumotlar markazi uchun to'g'ri joyni tanlash juda muhimdir. Elektr stantsiyalari, zilzila yoriqlari va tabiiy ofatlarga moyil bo'lgan hududlar yaqinidagi joylardan saqlaning. To'siqlar va xavfsizlik darvozalari kabi to'siqlarni amalga oshirish jismoniy xavfsizlikni yanada kuchaytiradi. Atrof-muhit nazorati ham muhim ahamiyatga ega. Bunga yong'inni o'chirish tizimlari, iqlim nazorati va ortiqcha quvvat manbalari kiradi. Ushbu chora-tadbirlar jismoniy tahdidlar ma'lumotlar markazingiz faoliyatini buzmasligini ta'minlaydi.

FOYDALANILGAN ADABIYOTLAR RO’YHATI:

1. **Shmatikov, V.** *Security and Privacy in Location-Based Services.* – Cornell University, 2007. *(Available at: Cornell University)*

2. **Santana, G. A. A.** *Data Center Virtualization Fundamentals.* – ISBN: 978-0134202663, 2016. *(Available at: WorldCat)*
3. **Federal Bureau of Investigation (FBI).** *The FBI 2003 Internet Fraud Report.* – Firenet Ltd, 2003. *(Available at: Firenet Ltd)*
4. **U.S. Department of State.** *Cybercrime Prevention and Detection: A Practical Guide.* – State.gov, 2023. *(Available at: State.gov)*
5. **Singer, P. W., & Friedman, A.** *Cybersecurity and Cyberwar: What Everyone Needs to Know.* – ISBN: 978-0199918119, 2014.

FOYDALANILGAN INTERNET SAHIFALARI:

1. https://www.interpol.int/Crimes/Cybercrime
2. https://www.state.gov/cybercrime
3. https://www.fbi.gov/investigate/cyber
4. https://community.fs.com/article/data-center-network-security-threats-and-solutions.html
5. https://www.cisco.com/c/en/us/solutions/security/secure-data-center-solution/what-is-data-center-security.html
6. https://www.cisco.com/c/en/us/solutions/collateral/enterprise/design-zone-security/safe-secure-cloud-architecture-guide.html
7. https://serverlift.com/blog/7-common-security-threats-for-data-centers/
8. https://www.checkpoint.com/cyber-hub/cyber-security/what-is-data-center/data-center-threats-and-vulnerabilities/#SecureYourDataCenter
9. https://www.nexusgroup.com/what-is-data-center-security/
10. https://learn.microsoft.com/en-us/compliance/assurance/assurance-threat-vulnerability-risk-assessment
11. https://en.wikipedia.org/wiki/Data_center_security