BULUTLI TEXNOLOGIYALARDA XAVFLARNI BOSHQARISH

I.S.Olimov [1], A.A.Karimov [1*], X.I. Ibrohimov [1]
[1,2,1]Tashkent university of information technologies named after Muhammad al- Khwarizmi
E-mail: karimovabduqodir041@gmail.com

Annotatsiya. *Ushbu maqolada Bulutli xavfni boshqarish to‘g‘risida ma`lumotlar yoritib berilgan. Bulutli axborot tizimlari tahdidlarga duchor bo'ladigan tashkilot faoliyatiga salbiy ta'sir ko'rsatishi mumkin (ya'ni, missiyalar, funktsiyalar, imidj yoki obro'), tashkilot aktivlari, jismoniy shaxslar va boshqa tashkilotlar. Risklarni boshqarish davriy ravishda amalga oshirilishi kerak bo`lgani uchun muvofiqlashtirilgan tadbirlar majmuini o'z ichiga olgan jarayon xavflarni nazorat qilishga asoslangan.*

Kalit so‘zlar. *Bulutli provayderlar, Risklarni boshqarish, SDLC, RMF*

KIRISH

Bulutli provayderlar eng zamonaviy bulutli ekotizimlarni taklif qilish imkoniyati, chidamli va xavfsiz - o'z tizimlarini boshqaradigan iste'molchilar muhitiga qaraganda ancha xavfsizroq tizimdir. Saqlangan ma'lumotlarning sezgirligi xavfsizlik va maxfiylikka qarshi ko'rib chiqilishi kerak bo’lgan yuzaga kelgan xavflar: Misol uchun, bulutga asoslangan afzalliklar yechim bulut modeliga, bulut turiga bog'liq bo'ladi, ko'rib chiqilgan xizmat, jalb qilingan ma'lumotlar turi, tizim tanqidiylik/ta'sir darajasi, xarajatlarni tejash, xizmat turi, va har qanday tegishli normativ talablar. Bulutli axborot tizimlari tahdidlarga duchor bo'ladigan tashkilot faoliyatiga salbiy ta'sir ko'rsatishi mumkin (ya'ni, missiyalar, funktsiyalar, imidj yoki obro'), tashkilot aktivlari, jismoniy shaxslar va boshqa tashkilotlar.

Zararli shaxslar ma'lum va noma'lum narsalardan foydalanishlari mumkin: maxfiylik, yaxlitlikni buzish uchun zaifliklar, yoki qayta ishlanayotgan, saqlanayotgan ma'lumotlarning mavjudligi,yoki ushbu tizimlar orqali uzatiladi.

Tashkilotlarga kerak bo'lgan ko'plab xavf turlari mavjud: dasturni boshqarish, investitsiyalar, byudjet, huquqiy javobgarlik, xavfsizlik, inventarizatsiya, ta'minot zanjiri, xavfsizlik va boshqalar. Risklarni boshqarishni har bir jihatga to'liq integratsiyalashgan yaxlit faoliyat sifatida ko'rish mumkin. Xatarlarni boshqarish faoliyati darajasiga qarab uch toifaga bo'lingan, ular xavf bilan bog'liq muammolarni hal qiladi:

1. Tashkilot darajasi (1-darajali)

2. Missiya va biznes jarayoni darajasi (2-darajali)
3. Axborot tizimi darajasi (3-darajali)

Risklarni boshqarish davriy ravishda amalga oshirilishi kerak bo`lgani uchun muvofiqlashtirilgan tadbirlar majmuini o'z ichiga olgan jarayon xavflarni nazorat qilishga asoslangan. Bu jarayon maqsadli strategik va taktik xavfsizlikni kuchaytirish va xavfni baholashni amalga oshirish, xavfni kamaytirish strategiyasini amalga oshirish va ishga joylashishni o'z ichiga oladi. Xavflarni nazorat qilish texnikasi va axborot xavfsizligi holatini doimiy monitoring qilish tartib-qoidalari tizimi. Bulutli axborot tizimlari, an'anaviy axborot tizimlari kabi, xavflarni boshqarishni talab qiladi. Butun tizimni ishlab chiqish hayotiy tsikli (SDLC).

Ushbu mavzuda biz faqat 3-darajali xavfsizlik xavfiga e'tibor qaratami. Bulutga asoslangan axborot tizimlarining ishlashi va ulardan foydalanish bilan bog'liq bo`lgan har qanday tahdidlarning oldini olish va yumshatish uchun, salbiy harakatlar, xizmat ko'rsatishdagi uzilishlar, hujumlar yoki murosalar uchun tashkilotlar o'zlarining qoldiq xavfini hisoblashlari kerak. Qabul qilinadigan xavf darajasidan past,Axborot tizimlari risklarini boshqarish (3-darajali xavf menejment) 1-darajali tavakkalchilik qarorlari asosida boshqariladi va 1 va 2-darajali xavf bo'yicha qarorlar yakuniy natijaga ta'sir qiladi,ularning asosida tashkilot tizimlarini tanlash, ma’lumotlar sezgirligi, mos bulut arxitekturasi va himoya choralari va qarshi choralar (ya'ni, xavfsizlik boshqaruv organlari) axborot tizimi darajasida. Ma`lumotni tanlash orqali xavfsizlik talablari qondiriladi, tegishli boshqaruv, operatsion va texnik xavfsizlik va nazorat qilishning standartlashtirilgan kataloglaridan xavfsizlik nazorati (ya'ni, AQSh Milliy institute Standartlar va Texnologiyalar (NIST) maxsus nashri 800-53 Revizyon 4, ISO/IEC 27001, ISO/IEC 27002 va boshqalar).Bulutli ekotizimda o'zaro murakkab munosabatlar bulutli aktyorlar, aktyorlarning individual missiyalari, biznes jarayonlari va ularni qo'llab-quvvatlovchi axborot tizimlari talab qiladi.Barcha bulutli ishtirokchilarning ehtiyojlarini qondiradigan integratsiyalangan, ekotizim bo'ylab xavflarni boshqarish tizimi (RMF) kabi bulutga asoslangan ma'lumot uchun har qanday axborot tizimi, bulutli aktyorlar ularni baholash uchun javobgardir.Ular tomonidan belgilangan chegaraga bog'liq bo'lgan maqubil xavf bulut ekotizimining qoldiq xavfiga eksponental.Axborot xavfsizligi xavfini samarali boshqarish ekotizim darajasida quyidagi yuqori darajadagi elementlar bo'lishi kerak ular:

• risklarni boshqarish bo'yicha mas'uliyatni belgilashning orkestratsiyasida ishtirok etgan bulutli aktyorlarga bulutli ekotizim. Ichki, har bir bulut aktyori zimmasiga yanada mas'uliyat yuklashi kerak yuqori martabali rahbarlar va vakillar.

Keng miqyosda bulutli ekotizimni yaratish xavf-xatarga bag'rikenglik va buning muloqoti haqida ma'lumotni o'z ichiga olgan holda, ularning xizmat ko'rsatish darajasi

bo'yicha kelishuvlari (SLA) orqali xavf-xatarlarga chidamlilik xavfga ta'sir qiluvchi qarorlar qabul qilish faoliyati bag'rikenglik.

• Deyarli real vaqtda monitoring, tanib olish va har bir bulut ishtirokchisi tomonidan operatsiyadan kelib chiqadigan axborot xavfsizligi xavflarini tushunish yoki axborot tizimidan foydalangan holda foydalanish bulutli ekotizimdir.

• Bulutli ishtirokchilarning javobgarligi va bulutli ishtirokchilarning hodisalari, tahdidlari, risklarni boshqarish qarorlari va real vaqt rejimiga yaqin axborot almashishi.

Risklarni boshqarish asosi.

Xavf ko'pincha ehtimollik funktsiyasi sifatida ifodalanadi salbiy oqibat yuzaga kelishini, bunday salbiy natijaning kattaligiga ko'paytiriladi. Axborot xavfsizligida ehtimollik tahdidlar funktsiyasi sifatida tushuniladi tizimga, foydalanish mumkin bo'lgan zaifliklarga va bu zaifliklarning oqibatlar ekspluatatsiya. Shunga ko'ra, xavfsizlik xavfini baholashga e'tibor qaratiladi, bulut ekotizimining qayerga zarar etkazayotganini aniqlash bo'yicha voqealar yuz berishi mumkin.

Axborotni boshqarishning xavfga asoslangan yondashuvi tizimlar - bu rejalashtirishdan tortib SDLC jarayonlarigacha, xavfsizlikni boshqarish vositalarini taqsimlashgacha bo'lgan tashkilotning barcha jabhalariga to'liq integratsiya qilinishi kerak bo'lgan yaxlit faoliyatdir.

Shu sababli, RMF axborot xavfsizligini birlashtiradigan intizomli va tuzilgan jarayonni ta'minlaydI.SDLCda risklarni boshqarish faoliyati. RMF asosan risklarni boshqarishda 3-darajada ishlaydi,lekin u 1-darajada ham o'zaro ta'sirga ega bo'lishi mumkin.2-darajali ba'zi bir misol o'zaro ta'sirlar taqdim etishni o'z ichiga oladi, davom etayotgan monitoringdan olingan fikr-mulohazalar bilan tavakkalchi ijrochi va ruxsat berish qarorlaridan; tarqatish vakolatli mansabdor shaxslarga yangilangan xavf ma'lumotlari axborot tizimi egalari, va hokazo.NIST Maxsus nashri (SP) 800-37 1-versiya xavfi boshqaruv jarayoni - hukumat tomonidan tekshiriladigan jarayon agentliklar va xususiy sektor tashkilotlari an'anaviy axborot tizimlari uchun eng yaxshi amaliyot sifatida ko`rsatilgasn. Aytilganidek NIST SP 800-37 Rev. 1 da, xavfni qo'llash bo'yicha qo'llanma federal axborot tizimlarini boshqarish tizimi: axborot tizimini belgilaydigan xavfsizlikning hayot aylanishiga yondashuv talablar har qanday tizim rivojlanishining muhim qismidir,jarayon va tizimni ishga tushirish bosqichida boshlanishi kerak. Xavfsizlik talablari umumiy funktsional va funktsional bo'lmagan talablarning bir qismi bo'lganligi sababli, xavfsizlik talablar funktsional va funktsional bo'lmagan talablar bilan bir vaqtda SDLC ga birlashtirilishi kerak. Xavfsizlik talablari aniqlanishi kerak va yechimlar tadqiq qilinishi va ishlab chiqilishi kerak tizim rivojlanishining boshlanishi. Xavfsizlikni tizimga qo'shimcha sifatida ko'rib chiqish va arxitektura va SDLC dan mustaqil echimlarni amalga oshirish bilan yuqori xarajatlarga

olib kelishi mumkin bo'lgan yanada qiyin jarayon xavfni samarali kamaytirish uchun past potentsialdir.

RMFni bulutli ekotizimda qo'llash bo'yicha joriy muhokama uchun bu erda foydalanilgan. Shuni ta'kidlash kerakki, NIST hujjati bo'lsa ham tashkil topgan murakkab axborot tizimlariga murojaat qiladi turli sub'ektlar tomonidan boshqariladigan bir nechta quyi tizimlar, u bulutga asoslangan axborot tizimlari yoki yordamchi dasturlarga asoslangan har qanday boshqa turdagi tizimlar resurslar.

Bulutga asoslangan axborot tizimi uchun bulut ekotizimini tashkil qilishda bulutli iste'molchilar, egalari sifatida tizim bilan bog'liq ma'lumotlardan tizim va ma'lumotlarning mutanosib ravishda xavfsizligini ta'minlash uchun javobgar bo'lib qoladi, ma'lumotlar sezgirligi bilan bulutli iste'molchilarning nazorat va to'g'ridan-to'g'ri boshqarish darajasi har xil bulutni joylashtirish modeliga asoslanadi [2]. RMF bilan parallel ravishda, funktsional stekning turli qatlamlari xizmat sifatida infratuzilma (IaaS) buluti, bulut iste'molchi funktsional stekning yuqori qismini boshqaradi gipervisordan yuqorida, iste'molchi esa Funktsional stek platformas-a-service (PaaS) buluti uchun mutanosib ravishda kamayadi va minimal darajaga kamayadi. Xizmat sifatida dasturiy ta'minot (SaaS) bulutli ekotizimida. Soddalashtirilgan holda faqat tashkilotchi tomonidan tashkil etilgan bulutli ekotizim modeli bulutli iste'molchi va bulut provayderi RMF bulutli provayder tomonidan qo'llaniladi.Bulutli iste'molchilar RMFni qo'llaydilar yuqori funktsional qatlamlar, qurilgan va joylashtirilganlar xizmat sifatida taqdim etilgan bulutli infratuzilmaning tepasida. Biroq, bulut xizmatini sotib olishdan oldin, bulut iste'molchi bilan bog'liq xavfni tahlil qilish kerak, ma'lum bir axborot tizimi uchun bulutga asoslangan yechimni qabul qilish va xavfni davolash va xavfni rejalashtirish ushbu tizimning bulutga asoslangan operatsiyalari bilan bog'liq faoliyatni boshqarish. Buning uchun bulutli iste'molchi kerak butun bulut ekotizimining istiqboliga ega bo'lgan bulutga asoslangan axborot tizimining ishlashiga xizmat qiladi. Bulutli iste'molchilar ham RMFni qo'llashlari kerak ularga imkon beradigan moslashtirilgan tarzda:

- Xatarlarni baholashni amalga oshiring
- Eng mos bulut arxitekturasini aniqlang
- Eng mos bulut xizmatini tanlang
- Bulut taklifida kerakli ko‘rinishga ega bo‘ling
- Zarur bo'lgan xavfni davolashni aniqlash va muzokaralar olib borish va

SLAni yakunlashdan oldin xavflarni nazorat qilishni yumshatish va xavfsizlik ruxsati bilan davom eting kabi jarayonlarni o'z ichiga olgan takrorlanadigan jarayon sifatida ko'rsatish.

Bulutli provayderning risklarni boshqarish jarayoni.

Bulutli provayderlar bulutli arxitekturani ishlab chiqadi va yaratadi, asosiy funktsiyalarni o'z ichiga olgan bulut xizmatlari va operatsion xususiyatlar, shu jumladan xavfsizlik va maxfiylik asosiy talablarga javob beradigan nazorat vositalari. Ularning yechimlari bulutning katta hovuzining ehtiyojlarini qondirishga qaratilgan iste'molchilarni minimal moslashtirishni talab qiladigan tarzda. Bulutli provayderni tanlash va amalga oshirish uning xavfsizlik va maxfiylik nazorati ularning samaradorligini, samaradorligini va tegishli cheklovlarni hisobga oladi.

Qonunlar, direktivalar, siyosatlar, standartlar yoki qoidalar bilan bulut provayderi bunga rioya qilishi kerak. Bulutli iste'molchilarning o'ziga xos talablari va vakolatlari ma'lum emas va shuning uchun umumiy yadro to'plami sifatida prognoz qilinadi.Bulutli provayderlar bulut nima ekanligini aniqlashda sezilarli moslashuvchanlikka ega xizmat va shuning uchun u bilan bog'liq chegara, tizim arxitektura va amalga oshirilgan vaqt, ular bulutli iste'molchilar ma'lumotlarining tabiatini qabul qiladilar. Shuning uchun xavfsizlik va maxfiylik nazorati bulutli provayder tomonidan tanlangan va amalga oshirilgan to'plamlar ko'p sonli potentsial iste'molchilarning ehtiyojlarini qondiradigan, taklif qilinadigan markazlashtirilgan tabiat bulut xizmati bulutli provayderga yuqori darajada muhandislik qilish imkonini beradiMaxsus xavfsizlik yechimlari an'anaviy IT tizimlariga qaraganda yuqori darajadagi xavfsizlik holatida [4]. Standartlashtirilgan yoki yaxshi tekshirilgan yondashuvlarni qo'llash bulut xizmati risklarini boshqarish muvaffaqiyat uchun juda muhimdir, bulutli ekotizim va uning qo'llab-quvvatlanadigan axborot tizimlari. Taklif etilayotgan bulut xizmati to'g'ridan-to'g'ri bo'lgani uchun bulut provayderi tomonidan boshqariladi va nazorat qilinadi, qo'llash RMF ushbu tizimga qo'shimcha vazifalarni talab qilmaydi, klassik IT tizimidan tashqari; Shuni ta'kidlash kerakki, a ning xavfsizlik pozitsiyasi bulutli ekotizim faqat eng zaif quyi tizim yoki funktsional qatlam kabi kuchli. Bulutli provayderning obro'si va biznesning uzluksizligi silliqlikka bog'liq ishlashi va ularning iste'molchilarining yuqori ishlashi echimlar, RMF bulutli provayderni qo'llashda ularning bulutidagi mumkin bo'lgan zaiflikni qoplashga qaratilgan iste'molchilarning echimlari [3,5].

Bulutli iste'molchining risklarni boshqarish jarayoni

Yuqori darajadagi nazorat tashkilotlarga muqobil variantlarni ko'rib chiqishga, ustuvorliklarni belgilashga va o'z manfaatlari yo'lida qat'iy harakat qilishga imkon beradi. Bulutga asoslangan axborot tizimi yechimini muvaffaqiyatli qabul qilish uchun bulutli iste'molchi tizimning bulutga xos xususiyatlarini, arxitektura komponentlarini aniq tushuna olishi kerak har bir xizmat turi va joylashtirish modeli va bulut Xavfsiz bulut ekotizimini yaratishda aktyorlarning roli.

Bundan tashqari, bu iste'molchilarning biznesini bulutli qilish uchun juda muhimdir va ular qobiliyatiga ega bo'lgan missiya-tanqidiy jarayonlar:

• Barcha bulutga xos, xavfga qarab sozlangan xavfsizlikni aniqlang va maxfiylik nazorati;

Bulutli provayderlar va brokerlardan so'rov - mavjud bo'lganda va shartnoma asosida vositalari-xizmat shartnomalari va SLA qaerda xavfsizlik va maxfiylik nazoratini amalga oshirish hisoblanadi bulut provayderlarining javobgarligi

• Ushbu xavfsizlikni amalga oshirishni baholash va maxfiylik nazorati;

• Barcha aniqlangan xavfsizlikni doimiy ravishda kuzatib boring va maxfiylik nazorati.

Bulutga asoslangan xizmatlarda ba'zi quyi tizimlar yoki quyi tizim komponentlari bulutning bevosita nazorati iste'molchi tashkiloti ostida qoladi. Chunki bulutga asoslangan yechimni qabul qilish tabiatan bir xil narsani ta'minlamaydi, xavfsizlik darajasi va mandatlarga muvofiqligi an'anaviy IT modeli, keng qamrovli xavflarni baholashni amalga oshirish qobiliyatiga ishonchni mustahkamlash uchun kalit hisoblanadi. Bulutga asoslangan tizim uni avtorizatsiya qilishda birinchi qadam sifatida operatsiya. Bulutli ekotizimning xususiyatlariga quyidagilar kiradi:

• Keng tarmoqqa kirish

• Bulutli iste'molchilar tomonidan ko'rinish va nazoratning pasayishi

• Dinamik tizim chegaralari va o'zaro bog'liq roller bulutli iste'molchi va o'rtasidagi mas'uliyat bulut provayderi

• Ko'p ijaraga olish

• Ma'lumotlar rezidentligi

• O'lchovli xizmat

Bu xususiyatlar ko'pincha bulutli iste'molchini ko'rsatadi an'anaviy axborot texnologiyalari yechimlaridagidan farq qiladigan xavfsizlik xatarlari bilan, saqlab qolish uchun ularning axborot tizimi va ma'lumotlarining xavfsizlik darajasi bulutga asoslangan yechim, bulutli iste'molchilar barcha bulutga xos, xavfga qarab sozlangan xavfsizlikni aniqlash qobiliyatiga muhtoj va maxfiylikni oldindan nazorat qiladi. Bulut provayderlari va brokerlaridan shartnomaviy vositalar va SLAlar orqali barcha xavfsizlik va maxfiylik komponentlari aniqlangan va ularning boshqaruvi to‘liq va aniq amalga oshirildi. Turli xil bulutli hisoblashlar o'rtasidagi munosabatlar va o'zaro bog'liqlikni tushunish joylashtirish modellari va xizmat ko'rsatish modellari uchun juda muhimdir.Turli xil xizmatlar kombinatsiyasini ta'minlash uchun usullar va mas'uliyatlardagi farqlar va joylashtirish modellari katta qiyinchilik tug'diradi.Ular xavfni to'liq baholashlari kerak, xavfsizlik va maxfiylik boshqaruvlarini aniq aniqlash xavfni davolash jarayonining bir qismi sifatida atrof-muhitning xavfsizlik darajasini

saqlab qolish va bulutga o'tgandan keyin operatsiyalar va ma'lumotlarni kuzatish uchun zarur [1].

Bulutli iste'molchilar hozirda qaysi bulut xizmatini aniqlashda bir qancha qiyinchiliklarga duch kelishmoqda. Umuman olganda, bulutli iste'molchi bulutga asoslangan yechim quyidagi bosqichlarni bajarishi kerak:

1. Qaysi xizmat yoki ilovani tavsiflang bulutga asoslangan yechimdan foydalanish mumkin;

2. Bo'lishi kerak bo'lgan barcha funktsional imkoniyatlarni aniqlang ushbu xizmat uchun amalga oshiriladi;

3. Xavfsizlik va maxfiylik talablarini aniqlang va xizmatni himoya qilish uchun zarur bo'lgan xavfsizlik boshqaruvlari yoki ilova NIST standartlari va ko'rsatmalarini qabul qiluvchilar uchun, bulutli iste'molchilar axborot tizimlarining xavfsizlik toifasini va tegishli ta'sir darajasini aniqlashlari kerak bo`ladi;

Xulosa

Xulosa qilib aytganda, bulutga asoslangan yechimni qabul qilish axborot tizimi bulutli iste'molchilarni talab qiladi. Ularning xavfsizlik talablarini sinchkovlik bilan aniqlash, baholash har bir bo'lajak xizmat ko'rsatuvchi provayderning xavfsizligi va maxfiyligi nazorat qiladi. Bulutga asoslangan xizmatlarda ba'zi quyi tizimlar yoki quyi tizim komponentlari bulutning bevosita nazorati iste'molchi tashkiloti ostida qoladi. Chunki bulutga asoslangan yechimni qabul qilish tabiatan bir xil narsani ta'minlamaydi, xavfsizlik darajasi va mandatlarga muvofiqligi an'anaviy IT modeli, keng qamrovli xavflarni baholashni amalga oshirish qobiliyatiga ishonchni mustahkamlash uchun kalit hisoblanadi

FOYDALANILGAN ADABIYOTLAR

1. Karimov, Abdukodir, et al. "Cloud Computing Security Challenges and Solutions." *2021 International Conference on Information Science and Communications Technologies (ICISCT)*. IEEE, 2021.
2. Sun, PanJun. "Security and privacy protection in cloud computing: Discussions and challenges." *Journal of Network and Computer Applications* 160 (2020): 102642.
3. Tabrizchi, Hamed, and Marjan Kuchaki Rafsanjani. "A survey on security challenges in cloud computing: issues, threats, and solutions." *The journal of supercomputing* 76.12 (2020): 9493-9532.
4. Sasubilli, Manoj Kumar, and R. Venkateswarlu. "Cloud computing security challenges, threats and vulnerabilities." *2021 6th international conference on inventive computation technologies (ICICT)*. IEEE, 2021.
5. Shabbir, Maryam, Ayesha Shabbir, Celestine Iwendi, Abdul Rehman Javed, Muhammad Rizwan, Norbert Herencsar, and Jerry Chun-Wei Lin. "Enhancing security of health information using modular encryption standard in mobile cloud computing." *IEEE Access* 9 (2021): 8820-8834.