BULUTLI TEXNOLOGIYALARDAGI ELEKTRON HUJJATLARGA QARATILGAN TAHDIDLAR

Fayziyeva Dilsora TATU



Annotatsiya

Ushbu maloqada bulutli texnologiyalar hususiyatlari, turlari va unda saqlanadigan electron hujjatlarga qaratilgan tahdidlar va tahdid manbalari keltirib o‘tilgan.

Kalit so‘zlar: zararli insayderlar, DoS va DDoS hujumlari, CSA

Аннотация

В данном статье упомянуты характеристики и виды облачных технологий, а также угрозы и источники угроз хранящимся в них электронным документам.

Ключевые слова: злонамеренные инсайдеры, DoS и DDoS-атаки, CSA

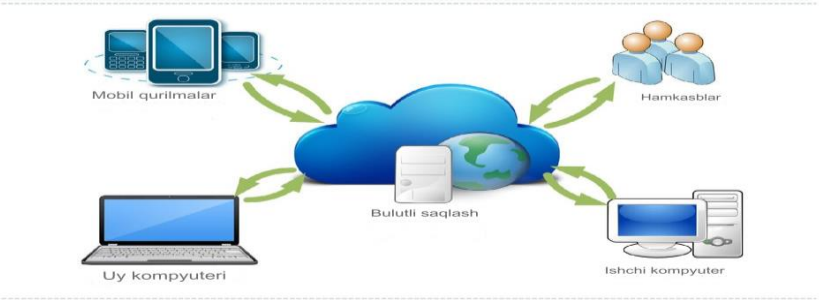
Annotation

In this report, the characteristics and types of cloud technologies, as well as threats and sources of threats to electronic documents stored in them, are mentioned.

Keywords: malicious insiders, DoS and DDoS attacks, CSA

Bulutli texnologiyalar xususiyatlarining juda ko'p ta'riflari va tavsiflari mavjud. Shunga ko'ra, bulutli texnologiya - bu minimal operatsion xarajatlar va/yoki xizmat ko'rsatuvchi provayderning resursi bilan tez ta'minlanishi va chiqarilishi mumkin bo'lgan umumiy konfiguratsiya qilinadigan hisoblash resurslariga hamma joyda va qulay talab bo'yicha tarmoq kirishini ta'minlash modeli. Bulutli hisoblashning dolzarbligi masalasini ko'targan holda, ushbu xizmatlar bozorining o'sish statistikasi, prognozlar va asosiy yo'nalishlarni amalga oshirishni eslatib o'tish kerak. Ishonch bilan aytish mumkinki, barcha zamonaviy Internet foydalanuvchilari bulutli xizmatlardan foydalanadilar, ulardan eng mashhurlari xosting, elektron pochta va ijtimoiy tarmoqlardir. Ushbu texnologiyaning asosiy afzalliklari egiluvchanlik - resurslarni masshtablash qobiliyati, iqtisodiy samaradorlik va samaradorlik, ishonchlilik, ma'lumotlarga masofadan kirish. Hozirgi vaqtda bulutli xizmatlarni taqdim etish bo'yicha gigantlar Amazon EC2 va S3, Microsoft Azure, IBM Smart Cloud, OpenStack va boshqalar hisoblanadi. Bulutli texnologiyalar yetakchi mamlakatlarda hukumat darajasida qo‘llab-quvvatlanadi. Bulutli hisoblash texnologiyalarining istiqboli va iqtisodiy samaradorligi davlat darajasida ham e’tirof etilgan – dunyoning yetakchi mamlakatlari bulutli texnologiyalarni rivojlantirish bo‘yicha o‘z dasturlariga ega. Masalan, Rossiyada "Axborot jamiyati (2011 - 2020)" dasturi, xususan, bulutli texnologiyalarni rivojlantirishni ta'minlaydi. AQShda bulutli hisoblashni davlat darajasida amalga oshirish bo'yicha tavsiyalarni o'z ichiga olgan "Federal Cloud Computing Strategy" maxsus hujjati ishlab chiqilgan. Yaponiyada “Kasumigaseki Cloud” davlat sektori uchun ommaviy bulut infratuzilmasini yaratish loyihasi ishlab chiqildi. Hozirgi vaqtda texnologiya ko'plab uzoq vaqtdan beri ma'lum bo'lgan texnologiyalarning asoslarini to'pladi - xizmatga yo'naltirilgan arxitektura, WEB 2.0, virtualizatsiya va aytish mumkinki, autsorsingning tabiiy davomi. Uning afzalliklariga qaramay, texnologiya jiddiy kamchiliklarga ega. Bulutli hisoblashda axborot xavfsizligi muammosi davlat va global darajadagi jiddiy o'zgarishlarda ularni amalga oshirishni cheklovchi omillardan biridir. Muhim masala bulut tizimlarida xavflarni boshqarishdir. Foydalanuvchi, birinchi navbatda, xizmat ko'rsatish shartnomasining (SLA) barcha jihatlarini, shu jumladan xavfsizlik uchun javobgarlik sohasini tahlil qilishi kerak. 2010 yilda ISACA tomonidan o'tkazilgan so'rov bir qator qiziqarli tendentsiyalarni aniqladi. So‘rovda qatnashgan jami IT-mutaxassislarining 45 foizi xavf-xatarlar foydadan ancha ustun ekanligiga ishonadi va faqat 10 foizi muhim ilovalarni bulutga ko‘chirishni ko‘rib chiqishga tayyor. Xizmat foydalanuvchisi ko'pincha o'z ma'lumotlari qayerda joylashganligini yoki qayerga ko'chirilishi mumkinligini bilmaydi va shaxsiy ma'lumotlarni mamlakatdan tashqariga ko'chirish ba'zi hollarda maxfiylikning buzilishi bo'lishi mumkinligi sababli, bu jiddiy muammodir. Yana bir muhim muammo shundaki, texnologiya resurslarni almashish (ko‘p ijara muddati) va ma’lumotlarni, shu jumladan moliyaviy ma’lumotlarni bir joyda markazlashtirilgan holda ko‘p sonli foydalanuvchilarga joylashtirishni nazarda tutadi. Bunday holda, biz tajovuzkorlarning ularga kirishga qiziqishini istisno qila olmaymiz. Bulutli tizim

provayderlari foydalanuvchilarini oldindan aniqlay olmasligini unutmasligimiz kerak. Ularga yaxshi niyatli shaxslar ham, yomon niyatli shaxslar ham kirishi mumkin.



1-rasm. Bulutli saqlash tizimlariga qaratilgan tahdid manbalari

Misol uchun, xavfsizlik tadqiqotchilari Amazon EC2 serverlarida ishlaydigan botnetlar uchun parollarni o'g'irlash uchun Zeus botnetini topdilar. Xakerlar Amazon serverlarida joylashgan veb-saytni buzib, keyin yashirincha infratuzilmani boshqarish va boshqarishni o'rnatdilar. Bulutli texnologiyalarga turli tashqi hujumlar amalaga oshiriladi. 1-rasmda umumiy ko‘rinishi keltirilgan.

So'nggi yillarda bulutli texnologiyalar tobora ommalashib bormoqda: ko'plab kompaniyalar o'z xizmatlarini bulutli saqlashga o'tkazmoqda va muhim ma'lumotlarni joylashtirish uchun provayder bulutlaridan foydalanmoqda. Ushbu yechim iloji boricha amaliy va arzon bo'lib tuyuladi, ammo uni ishlatish jarayonida yuzaga kelishi mumkin bo'lgan muammolar haqida unutmaslik erak.

Bulutli migratsiyalar soni har yili o'sib bormoqda, bunday yechimlarning ishlashi va funksionalligi yaxshilanmoqda, ammo xavfsizlik masalasi hali ham o'tkirligicha qolmoqda. Bulutli texnologiyalarning xavfsizligi qanday ta'minlanganligi va ularning ishlashi davomida qanday muammolarga duch kelish mumkinligini o‘rganish dolzarb sanaladi.

1-tahdid. Ma'lumotlarning sizib chiqishi Bulut an'anaviy infratuzilmalar kabi tahdidlarga duchor bo'ladi. Bugungi kunda bulutlarga tez-tez uzatiladigan katta hajmdagi ma'lumotlar tufayli, bulutli hosting provayderlarining saytlari tajovuzkorlar uchun jozibali nishonga aylanadi. Bundan tashqari, potentsial tahdidlarning jiddiyligi bevosita saqlangan ma'lumotlarning ahamiyatiga bog'liq. Shaxsiy foydalanuvchi ma'lumotlarini oshkor qilish, qoida tariqasida, tibbiy hisobotlarni, tijorat sirlarini yoki intellektual mulkni oshkor qilishdan ko'ra, alohida kompaniyaning obro'siga jiddiy zarar etkazadigan kamroq oshkoralikni oladi. Ma'lumotlar sizib chiqqan taqdirda, tashkilot jarimalar, da'volar yoki jinoiy javobgarlikka tortiladi, shuningdek, brendga zarar etkazish va biznes yo'qotishlari ko'rinishidagi bilvosita tarkibiy qismlarga duch keladi, bu esa qaytarib bo'lmaydigan oqibatlarga olib keladi va kompaniya imidjini tiklash uchun uzoq protseduralar talab etadi. Shu sababli, bulutli provayderlar bulutli muhitda ma'lumotlarni to'g'ri nazorat qilish va himoya qilishni ta'minlashga harakat qilishadi. Ma'lumotlarning sizib chiqishi xavfi va tahdidlarini minimallashtirish uchun CSA ko'p faktorli autentifikatsiya va shifrlashdan foydalanishni tavsiya qiladi.

2-tahdid. Hisobni buzish va autentifikatsiyani chetlab o'tish Ma'lumotlarning buzilishi ko'pincha autentifikatsiya qilishning zaif mexanizmlari, zaif parollar va shifrlash kalitlari va sertifikatlarini yomon boshqarish natijasidir. Bundan tashqari, tashkilotlar huquqlar va ruxsatlarni boshqarish muammolariga duch kelishadi, bunda oxirgi foydalanuvchilarga zarur bo'lgandan ko'ra ko'proq ruxsatlar beriladi. Muammo, shuningdek, foydalanuvchi boshqa lavozimga o'tkazilganda yoki undan chiqib ketganda paydo bo'ladi. Ko'pchilik yangi foydalanuvchi rollariga ko'ra ruxsatlarni yangilashga shoshilmoqda. Natijada, hisob talab qilinganidan ko'ra ko'proq imkoniyatlarni o'z ichiga oladi. Va bu xavfsizlik nuqtai nazaridan qiyinchilik.

3-tahdid. Interfeyslarni va APIlarni buzish. Bugungi kunda bulutli xizmatlar va ilovalarni qulay foydalanuvchi interfeysisiz tasavvur qilib bo'lmaydi. Bulutli xizmatlarning xavfsizligi va mavjudligi APIda kirishni boshqarish va shifrlash mexanizmlari qanchalik yaxshi rivojlanganiga bog'liq. O'z API-larini ishlatadigan uchinchi tomon bilan o'zaro aloqada bo'lganda, xavflar sezilarli darajada oshadi. Chunki qo'shimcha ma'lumotlarni, jumladan, foydalanuvchining login va parolini

taqdim etish talab etiladi. Xavfsizlik zaif interfeyslar mavjudlik, maxfiylik, yaxlitlik va xavfsizlik nuqtai nazaridan to'siqlarga aylanadi.

CSA xavfsizlik va tahdidlarni erta aniqlash vositalaridan foydalangan holda tegishli kirish nazoratini tashkil qilishni tavsiya qiladi. Tahdidlarni modellashtirish va ularni qaytarish uchun echimlarni topish qobiliyati xakerlik hujumiga qarshi munosib profilaktika hisoblanadi. Bundan tashqari, CSA kod xavfsizligini tekshirishni va kirish testlarini o'tkazishni tavsiya qiladi.

4-tahdid. Foydalanilgan tizimlarning zaifligi. Amaldagi tizimlarning zaifligi ko'p ijarachili bulutli muhitda uchraydigan muammodir. Yaxshiyamki, u to'g'ri tanlangan IT boshqaruv usullari bilan minimallashtiriladi, deydi CSA. Eng yaxshi amaliyotlar qatoriga zaifliklarni muntazam ravishda skanerlash, so'nggi yamoqlarni qo'llash va xavfsizlik tahdidlari haqidagi xabarlarga tezkor javob berish kiradi. CSA hisobotlariga ko'ra, tizim zaifliklarini yumshatish uchun sarflangan xarajatlar boshqa IT xarajatlariga nisbatan pastroq. IaaS modelida bulutli yechimlardan foydalanishda keng tarqalgan xatolik shundaki, kompaniyalar bulutli provayderning xavfsiz infratuzilmasida joylashgan o‘z ilovalari xavfsizligiga yetarlicha e’tibor bermaydilar. Ilovalarning zaifligi esa korporativ infratuzilma xavfsizligida to'siq bo'lib qoladi.

5-tahdid. Hisobni o'g'irlash. Bulutda fishing, firibgarlik va ekspluatatsiyalar ham uchraydi. Bu erda tranzaktsiyalarni manipulyatsiya qilish va ma'lumotlarni o'zgartirishga urinishlar shaklida tahdidlar qo'shiladi. Bulutli platformalar tajovuzkorlar tomonidan hujumlarni amalga oshirish uchun maydon sifatida qabul qilinadi. Va hatto "chuqur mudofaa" strategiyasiga rioya qilish ham etarli bo'lmasligi mumkin. Foydalanuvchi hisoblari va xizmatlarini o'zaro "almashish" ni taqiqlash, shuningdek, ko'p faktorli autentifikatsiya mexanizmlariga e'tibor berish kerak. Xizmat hisoblari va foydalanuvchi hisoblari bajarilgan operatsiyalarni batafsil kuzatish bilan kuzatilishi kerak. Asosiysi, hisoblaringiz o'g'irlikdan himoyalanganligini ta'minlash, CSA tavsiya qiladi.

6-tahdid. Zararli insayderlar. Insayder tahdidi hozirgi yoki sobiq xodimlar, tizim ma'murlari, pudratchilar yoki biznes hamkorlardan kelib chiqishi mumkin. Yovuz niyatli insayderlar turli maqsadlarga ega bo'lib, ma'lumotlarni o'g'irlashdan tortib oddiygina qasos olishga qadar. Bulutli holatda, maqsad infratuzilmani to'liq yoki qisman yo'q qilish, ma'lumotlarga kirish va hokazo bo'lishi mumkin. Bulutli provayderning xavfsizligiga bevosita bog'liq bo'lgan tizimlar katta xavf hisoblanadi. CSA shifrlash mexanizmlari haqida g'amxo'rlik qilishni va shifrlash kalitlarini boshqarishni nazorat qilishni tavsiya qiladi. Shaxsiy hisoblar uchun hodisalarni ro'yxatga olish, kuzatish va tekshirish haqida unutmang.

7-tahdid. Maqsadli kiberhujumlar. Rivojlangan doimiy tahdid yoki maqsadli kiberhujum hozirgi kunlarda kam uchraydi. Etarli bilim va tegishli vositalar to'plami bilan siz natijalarga erishishingiz mumkin. Maqsadli infratuzilmada o'z mavjudligini o'rnatish va o'rnatishga kirishgan tajovuzkorni aniqlash unchalik oson emas. Xatarlarni minimallashtirish va bunday tahdidlarning oldini olish uchun bulutli xizmat ko'rsatuvchi provayderlar ilg'or xavfsizlik vositalaridan foydalanadilar. Ammo zamonaviy echimlarga qo'shimcha ravishda, ushbu turdagi hujumning mohiyati va tabiatini tushunish kerak. CSA xodimlarga tajovuzkor texnikasini tan olish, ilg'or xavfsizlik vositalaridan foydalanish, jarayonlarni to'g'ri boshqarish, rejalashtirilgan hodisalarga javob berishdan xabardor bo'lish va infratuzilma xavfsizligi darajasini oshiradigan oldini olish usullarini qo'llash uchun maxsus treningni tavsiya qiladi.

8-tahdid. Doimiy ma’lumotlar yo‘qolishi Bulutlar pishib qolganda, xizmat ko‘rsatuvchi provayder tufayli doimiy ma’lumotlar yo‘qolishi holatlari juda kam uchraydi. Shu bilan birga, tajovuzkorlar ma'lumotlarni doimiy ravishda o'chirish oqibatlarini bilib, bunday buzg'unchi harakatlarni amalga oshirishni maqsad qiladi. Xavfsizlik choralariga rioya qilish uchun bulutli hosting provayderlari foydalanuvchi ma'lumotlarini dastur ma'lumotlaridan ajratib, ularni turli joylarda saqlashni tavsiya qiladi. Zaxiralashning samarali usullari haqida unutmang. Har kuni zahira nusxalari va zahira nusxalarini tashqi muqobil xavfsiz saytlarda saqlash bulutli muhitlar uchun ayniqsa muhimdir. Bundan tashqari, agar mijoz ma'lumotlarni bulutga joylashtirishdan oldin shifrlasa, shifrlash kalitlarini saqlash xavfsizligi haqida oldindan g'amxo'rlik qilish kerak. Ular tajovuzkorning qo'liga tushishi bilan, ma'lumotlarning o'zi ular bilan birga bo'ladi, ularning yo'qolishi jiddiy oqibatlarga olib kelishi mumkin.

9-tahdid. Ogohlikning yetishmasligi

Bulutli imkoniyatlarni tushunmasdan bulutga o'tadigan tashkilotlar xavf-xatarlarga duch kelishadi. Agar, masalan, mijozning ishlab chiqish guruhi bulutli texnologiyalarning xususiyatlari va bulutli ilovalarni joylashtirish tamoyillari bilan etarlicha tanish bo'lmasa, operatsion va arxitektura muammolari paydo bo'ladi.

CSA sizga xizmat ko'rsatuvchi provayderingiz tomonidan taqdim etilgan bulut xizmatlarining ishlashini tushunishingizni eslatadi. Bu hosting provayderi bilan shartnoma tuzishda kompaniya qanday xavf-xatarlarni o'z zimmasiga oladi degan savolga javob berishga yordam beradi.

10-tahdid. Bulutli xizmatlardan suiiste'mol qilish

Bulutlar qonuniy va noqonuniy tashkilotlar tomonidan ishlatilishi mumkin. Ikkinchisining maqsadi zararli harakatlarni amalga oshirish uchun bulutli resurslardan foydalanish: DDoS hujumlarini boshlash, spam yuborish, zararli kontentni tarqatish va boshqalar. Xizmat ko'rsatuvchi provayderlar bunday ishtirokchilarni taniy olishlari juda muhim, buning uchun o'rganish tavsiya etiladi. traffikni batafsil va bulutli monitoring vositalaridan foydalaning.

11-tahdid: DDoS hujumlari. DoS hujumlari uzoq tarixga ega bo'lsa-da, bulutli texnologiyalarning rivojlanishi ularni yanada keng tarqalgan holga keltirdi. DoS hujumlari natijasida kompaniya biznesi uchun muhim bo'lgan xizmatlarning ishlashi sezilarli darajada sekinlashishi yoki butunlay to'xtatilishi mumkin. Ma'lumki, DoS hujumlari katta hajmdagi hisoblash quvvatini sarflaydi, undan foydalanish uchun mijoz to'laydi. DoS hujumlari tamoyillari bir qarashda oddiy bo'lishiga qaramay, ularning amaliy darajasida xususiyatlarini tushunish kerak: ular veb-serverlar va ma'lumotlar bazalaridagi zaifliklarni nishonga oladi. Bulutli provayderlar, albatta, individual mijozlarga qaraganda, DoS hujumlari bilan kurashishda yaxshiroq. Eng muhimi, hujum sodir bo'lishidan oldin uni yumshatish rejasiga ega bo'lishdir.

12-tahdid. Qo'shma texnologiyalar, umumiy xavflar. Amaldagi texnologiyalardagi zaifliklar bulut uchun etarli darajada tahdiddir. Bulutli xizmat ko'rsatuvchi provayderlar virtual infratuzilmani, bulutli ilovalarni taqdim etadi, ammo agar qatlamlardan birida zaiflik yuzaga kelsa, u butun muhitga ta'sir qiladi. CSA tarmoq segmentatsiyasi kontseptsiyasiga va eng kam imtiyoz printsipiga rioya qilgan holda, ko'p faktorli autentifikatsiya mexanizmlarini, hujumlarni aniqlash tizimlarini amalga oshirishni, chuqur xavfsizlik strategiyasidan foydalanishni tavsiya qiladi.

Adabiyotlar ro‘yxati

1. U.M.Yarlakabov Didactic Ways of Forming Students' Technical Thinking.- Eastern European Scientific Journal, 2018 - journale.auris-verlag.de

2. Sharipov Sanjar. Vocational orientation through the development of mathematical competences in the students of technical higher education institutions. CURRENT RESEARCH JOURNAL OF PEDAGOGICS. 3. No. 06 (2022). 58-64. https://doi.org/10.37547/pedagogics-crjp-03-06-10

3. Nadirova-Kazan, H. (2023, November). EXPLORING THE CONTENT OF MEDIA LITERACY: A COMPREHENSIVE REVIEW. In International Scientific and Current Research Conferences (pp. 107-110).

4. Mahkamov, S., Aynakulov, T., & Baratov, J. (2024). ANDROIDDA MODEL VIEW PRESENTER (MVP) ARXITEKTURASI. International Journal of scientific and Applied Research, 1(3), 199-202.

5. Ikrom Kulanov, Sneha Latha, Azizbek Uzakboyev, Shakhzoda Burkhanova. Effect of gyrotactic microorganisms on electrically conducting carreau nanofluid flow along an exponentially stretching surface in the presence of chemical reaction. Problems in the textile and light industry in the context of integration of science and industry and ways to solve them: ptlicisiws-2.4–5 may 2023.Namangan, Uzbekistan.AIP Conf. Proc. 3045, 030066 (2024). https://doi.org/10.1063/5.0197498

6. Sanjar Sobirovich Sharipov. IMPLEMENTATION OF SPECIAL AND GENERAL PROFESSIONAL INTEGRATION AS A PEDAGOGICAL PROBLEM Scientific Bulletin of Namangan State University.2020. 2-8. 364-370-p.