BULUTLI TIZIMLARDA AXBOROTNI HIMOYALASHNING USULLARI

Мухаммад ал-Хоразмий номидаги ТАТУ Самарканд филиали
Бобобекова Х.Р. , Улугова Б.

Annotatsiya. Ushbu maqola bulut tizimlarida ma'lumotlarni himoya qilish usullarini o'rganadi. U bulutdagi ma'lumotlar xavfsizligi bilan bog'liq muammolar haqida umumiy ma'lumot beradi va xavflarni kamaytirish uchun turli strategiyalarni o'rganadi. Maqolada ma'lumotlarni shifrlash, kirishni boshqarish, ma'lumotlarni zaxiralash va kirishni aniqlash kabi muhim texnikalar hamda ularning maxfiy ma'lumotlarni himoya qilishdagi ahamiyati yoritilgan. Bulutli tizimlarda axborotni himoya qilishga kompleks yondashuv zarurligini ta'kidlash bilan yakunlanadi.

Kalit so'zlar: bulutli tizimlar, axborotni himoya qilish, ma'lumotlar xavfsizligi, bulutli hisoblash, ma'lumotlarni shifrlash, kirishni boshqarish, ma'lumotlarni zaxiralash, kirishni aniqlash.

Annotation. This article explores data protection techniques in cloud systems. It provides an overview of data security issues in the cloud and explores various strategies to reduce risks. The article covers important techniques such as data encryption, access control, data backup and access detection, as well as their importance in protecting confidential information. It concludes by highlighting the need for an integrated approach to Information Protection in cloud systems.

Keywords: Cloud Systems, Information Protection, data security, cloud computing, data encryption, access control, data backup, access detection.

Аннотация. В этой статье рассматриваются методы защиты данных в облачных системах. Он предоставляет обзор проблем безопасности данных в облаке и исследует различные стратегии снижения рисков. В статье рассматриваются важные методы, такие как шифрование данных, контроль доступа, резервное копирование данных и обнаружение вторжений, а также их важность для защиты конфиденциальных данных. В заключение подчеркивается необходимость комплексного подхода к защите информации в облачных системах.

Ключевые слова: облачные системы, защита информации, безопасность данных, облачные вычисления, шифрование данных, контроль доступа, резервное копирование данных, обнаружение доступа.

Bulutli hisoblash ma'lumotlarni saqlash va qayta ishlash uchun kengaytiriladigan va tejamkor echimlarni taklif qilish orqali korxonalarning ishlash usullarini inqilob qildi. Shu bilan birga, bulutli muhit nozik ma'lumotlarning himoyasini ta'minlash uchun hal qilinishi kerak bo'lgan turli xil xavfsizlik

muammolarini ham keltirib chiqaradi. Ushbu maqola bulutli tizimlarda axborotni himoya qilish usullarini o'rganishga, ma'lumotlar xavfsizligining muhimligini ta'kidlashga va bulutdagi ma'lumotlarni himoya qilish uchun ishlatilishi mumkin bo'lgan turli xil yondashuvlar va texnikalar haqida tushuncha berishga qaratilgan.

Ma'lumotlarni Shifrlash:Ma'lumotlarni shifrlash bulutli tizimlarda ma'lumotlarni himoya qilishning asosiy usuli hisoblanadi. Bu shifrlash algoritmlari yordamida ma'lumotlarni o'qib bo'lmaydigan formatga aylantirishni o'z ichiga oladi. Shifrlash ruxsatsiz tomonlar ma'lumotlarga kirish huquqiga ega bo'lsalar ham, tegishli shifrlash kalitlarisiz uni hal qila olmasliklarini ta'minlaydi. Kuchli shifrlash mexanizmlarini qo'llash tranzitda va bulut ichida dam olishda ma'lumotlarning maxfiyligini ta'minlashga yordam beradi.

Kirishni Boshqarish:Kirishni boshqarishning mustahkam mexanizmlarini joriy qilish maxfiy ma'lumotlarga ruxsatsiz kirishni oldini olish uchun juda muhimdir. Kirishni boshqarish autentifikatsiya, avtorizatsiya va audit jarayonlarini o'z ichiga oladi. Ma'lumotlarga kirishdan oldin foydalanuvchilar o'zlarini tasdiqlashlari kerak va ularning kirish huquqlari oldindan belgilangan avtorizatsiya siyosati asosida aniqlanishi kerak. Muntazam audit potentsial xavfsizlik buzilishlarini aniqlash va kamaytirishga yordam beradi.

Ma'lumotlarni zaxiralash va tiklash: Ma'lumotlarning yo'qolishi turli sabablarga ko'ra yuzaga kelishi mumkin, masalan, apparatdagi nosozliklar, tabiiy ofatlar yoki inson xatolari. Ma'lumotlarni zaxiralash va tiklashning keng qamrovli strategiyasini amalga oshirish bulutli tizimlardagi ma'lumotlarni himoya qilish uchun juda muhimdir. Muhim ma'lumotlarni saytdan tashqari joylarga yoki alohida bulutli serverlarga muntazam ravishda zaxiralash kutilmagan hodisalar yuz berganda ma'lumotlarni tiklashni ta'minlaydi.

Bulutli tizimlar ma'lumotlarning xavfsizligi va maxfiyligini ta'minlash uchun axborotni himoya qilishning turli usullarini qo'llaydi. Bu erda ishlatiladigan ba'zi umumiy usullar:

- Shifrlash: shifrlash-bu kriptografik algoritmlar yordamida ma'lumotlarni o'qib bo'lmaydigan formatga aylantirish jarayoni. Bulutli tizimlar ko'pincha ma'lumotlarni dam olishda (bulutda saqlangan) va tranzitda (bulut va foydalanuvchi qurilmalari o'rtasida uzatish paytida) himoya qilish uchun shifrlashdan foydalanadilar. Kuchli shifrlash, agar ma'lumotlar buzilgan bo'lsa ham, tegishli shifrlash kalitlarisiz tushunarsiz bo'lib qolishini ta'minlaydi.
- Kirishni boshqarish: kirishni boshqarish mexanizmlari Foydalanuvchining bulutli resurslar va ma'lumotlarga kirishini tartibga soladi va cheklaydi. Bunga autentifikatsiya (foydalanuvchi identifikatorlarini tekshirish), avtorizatsiya (rollar va imtiyozlar asosida tegishli ruxsatlarni berish) va audit (foydalanuvchi faoliyatini kuzatish va ro'yxatga olish) kiradi. Kirishni boshqarish bulut tizimidagi

ma'lumotlarga faqat vakolatli shaxslar kirishi va o'zgartirishi mumkinligini ta'minlaydi.

- Xavfsizlik devorlari: xavfsizlik devorlari bulut tizimi va tashqi tarmoqlar o'rtasida to'siq bo'lib, kiruvchi va chiquvchi tarmoq trafigini filtrlaydi. Ular ruxsatsiz kirishning oldini olishga yordam beradi va tarmoq hujumlari, zararli dasturlar va kirishga urinishlar kabi turli xil kiber tahdidlardan himoya qiladi. Xavfsizlik devorlari odatda faqat tasdiqlangan tarmoq trafigiga ruxsat berish va potentsial zararli yoki shubhali ulanishlarni blokirovka qilish uchun tuzilgan.
- Kirishni aniqlash va oldini olish tizimlari (IDP): IDPLAR potentsial xavfsizlik hodisalarini aniqlash va ularga javob berish uchun bulut muhitidagi tarmoq trafigini va tizim hodisalarini kuzatib boradi. Ushbu tizimlar ruxsatsiz kirishga urinishlar, zararli dastur infektsiyalari yoki shubhali xatti-harakatlar kabi zararli harakatlarni aniqlay oladi va tahdidlarni yumshatish uchun tegishli choralarni ko'radi. IDPLAR Real vaqtda ogohlantirishlar, jurnallarni tahlil qilish va xavfsizlik hodisalariga avtomatlashtirilgan javoblar kabi xususiyatlarni o'z ichiga olishi mumkin.
- Ma'lumotlarni zaxiralash va tiklash: bulutli tizimlar ko'pincha tasodifiy o'chirish, apparatdagi nosozliklar yoki tabiiy ofatlar tufayli ma'lumotlarni yo'qotishdan himoya qilish uchun ishonchli ma'lumotlarni zaxiralash va tiklash mexanizmlarini amalga oshiradi. Agar kerak bo'lsa, ma'lumotlarning avvalgi holatiga qaytarilishini ta'minlash uchun muntazam zaxira nusxalari amalga oshiriladi. Bu ma'lumotlar yaxlitligini va mavjudligini saqlashga yordam beradi.
- Xavfsizlikni kuzatish va ro'yxatga olish: bulutli tizimlar atrof-muhitdagi xavfsizlik hodisalari va faoliyatini kuzatib borish va qayd etish uchun keng qamrovli xavfsizlik monitoringi va ro'yxatga olish mexanizmlaridan foydalanadi. Bunga tarmoq trafigini kuzatish, foydalanuvchiga kirish, tizim konfiguratsiyasi va boshqa tegishli parametrlar kiradi. Xavfsizlik jurnallari hodisalarni tekshirish, sud-tibbiy tahlil qilish va xavfsizlikning potentsial zaifliklarini aniqlash uchun ishlatilishi mumkin.
- Zaiflikni baholash va Penetratsion test: bulut tizimidagi potentsial xavfsizlik kamchiliklarini aniqlash uchun muntazam ravishda zaifliklarni baholash va penetratsion testlar o'tkaziladi. Ushbu testlar tizimning mudofaasini baholash va takomillashtirishni talab qiladigan joylarni aniqlash uchun simulyatsiya qilingan hujumlar va zaifliklarni tekshirishni o'z ichiga oladi. Zaifliklarni faol ravishda hal qilish orqali bulut provayderlari o'z tizimlarining umumiy xavfsizlik holatini oshirishi mumkin.

Shuni ta'kidlash kerakki, ishlatiladigan maxsus usullar bulutli xizmat ko'rsatuvchi provayderga va tizimning o'ziga xos xavfsizlik talablariga qarab farq qilishi mumkin. Bulutli provayderlar odatda ushbu usullarning kombinatsiyasidan

foydalanadilar va o'z tizimlarida mustahkam axborot himoyasini ta'minlash uchun sanoatning eng yaxshi amaliyotlari va muvofiqlik standartlariga rioya qiladilar.

Yuqorida muhokama qilingan usullar bulutli tizimlarda axborotni himoya qilishga qatlamli yondashuvni ta'minlaydi. Kuchli ma'lumotlarni shifrlash, kirishni boshqarish choralarini qo'llash va ma'lumotlarni zaxiralash va tiklash protseduralarini amalga oshirish orqali tashkilotlar ma'lumotlarning buzilishi va ruxsatsiz kirish xavfini sezilarli darajada kamaytirishi mumkin.

Muhokama:

Yuqorida aytib o'tilgan usullar bulutli tizimlarda axborotni samarali himoya qilishni taklif qilsa-da, boshqa omillarni hisobga olish kerak. Bulutli xizmat ko'rsatuvchi provayderlar o'zlarining ma'lumotlar markazlarida mustahkam jismoniy va mantiqiy xavfsizlik choralarini saqlash kabi sanoatning eng yaxshi amaliyotlariga rioya qilishlari kerak. Potentsial tahdidlarni zudlik bilan aniqlash va yumshatish uchun muntazam ravishda xavfsizlik tekshiruvlari, zaifliklarni baholash va kirishni aniqlash tizimlari amalga oshirilishi kerak.

Xulosa va takliflar:

Bulutli tizimlarda axborotni himoya qilish maxfiy ma'lumotlarni himoya qilish uchun juda muhimdir. Tashkilotlar ma'lumotlarni shifrlash, kirishni boshqarish, ma'lumotlarni zaxiralash va tiklash mexanizmlarini o'z ichiga olgan kompleks yondashuvni qo'llashlari kerak. Shuningdek, ishonchli bulutli xizmat ko'rsatuvchi provayderlar bilan yaqindan ishlash va sohaga xos bo'lgan me'yoriy talablarga muvofiqligini ta'minlash juda muhimdir. Xodimlarni muntazam ravishda o'qitish va xabardor qilish dasturlari tashkilotning umumiy xavfsizlik holatini oshirishi mumkin.

Xulosa qilib aytganda, bulutli tizimlarda ma'lumotlarni himoya qilish texnik choralar, ilg'or tajribalarga rioya qilish va doimiy hushyorlikni talab qiladi. Ushbu maqolada muhokama qilingan usullarni qo'llash va rivojlanayotgan xavfsizlik tendentsiyalaridan xabardor bo'lish orqali tashkilotlar bulutli hisoblash bilan bog'liq xavflarni minimallashtirishi va doimiy rivojlanayotgan raqamli landshaftda o'zlarining qimmatli ma'lumotlarini himoya qilishi mumkin.

Eslatma: ushbu maqola faqat ma'lumot olish uchun mo'ljallangan va yuridik yoki professional maslahat sifatida qaralmasligi kerak. Tashkilotlar o'ziga xos bulutli muhitda axborotni himoya qilishga moslashtirilgan yondashuvni ishlab chiqish uchun xavfsizlik bo'yicha mutaxassislar va yuridik mutaxassislar bilan maslahatlashishlari kerak.

FOYDALANILGAN ADABIYOTLAR:

1. Абдулина Э.М. Облачные технологии в образовании // Молодой ученый. – 2019. – № 52 (290). – С. 7-9. – https://moluch.ru/archive/290/65873
2. Понятие «Облачные технологии» – https://studwood.ru/1046027/informatika/ponyatie_oblachnye_tehnologii
3. Облачные технологии: что это и как использовать бизнесу – https://blog.sibirix.ru/tech-clouds